PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-044141
(43)Date of publication of application : 08.02.2002

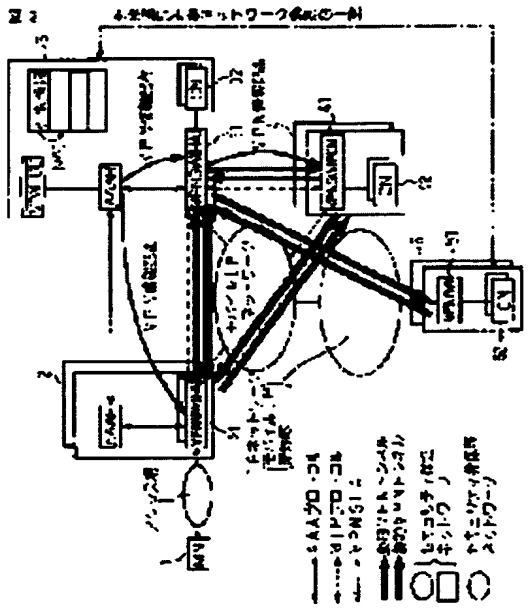
(51)Int.Cl. H04L 12/56
H04L 12/66
H04L 12/22

(21)Application number : 2000-225857
(22)Date of filing : 26.07.2000

(71)Applicant : FUJITSU LTD
(72)Inventor : KAKEMIZU MITSUAKI
YAMAMURA SHINYA
IGARASHI YOICHIRO
MURATA KAZUNORI
WAKAMOTO MASAAKI

(54) VPN SYSTEM IN MOBILE IP NETWORK AND SETTING METHOD FOR VPN

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a VPN(Virtual Private Network) service by an IPSec (tunnel) between optional terminals without providing of a special function for the VPN in interlocking with a position registration procedure in a mobile IP.
SOLUTION: The VPN system consists of mobile terminals, an authentication server, a VPN database and a network unit, and VPN information of a user requesting an authentication is extracted from the VPN database on position registration request from the mobile terminal, and the VPN system informs each network unit about the VPN information by using a prescribed position registration message and an authentication reply message. The network unit respectively set a VPN path in compliance with the IPSec between a home network unit and an external network unit, between the home network unit and a prescribed network unit and/or between the external network unit and the prescribed network unit on the basis of the reported VPN information.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－44141
（Ｐ2002－44141Ａ）
(43)公開日　平成14年２月８日(2002.2.8)

(51)Int.Cl.'	識別記号	ＦＩ	テーマコード'（参考）
Ｈ０４Ｌ　12/56		Ｈ０４Ｌ　11/20	１０２Ａ　５Ｋ０３０
12/66			Ｂ
12/22		11/26	

審査請求　未請求　請求項の数10　ＯＬ　（全 25 頁）

(21)出願番号　特願2000－225357(Ｐ2000－225357)
(22)出願日　平成12年７月26日(2000.7.26)

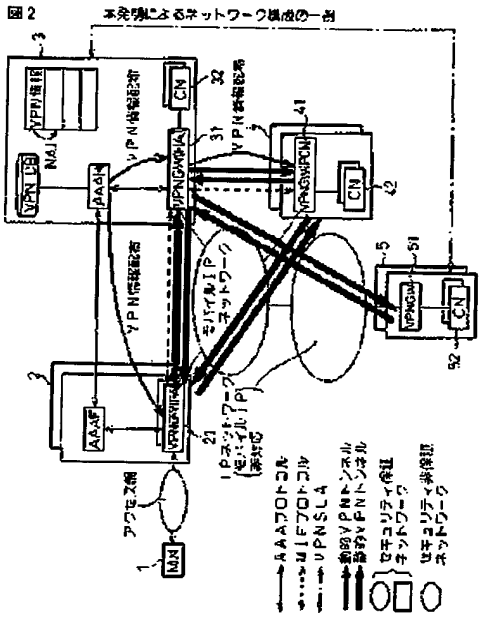
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　掛水　光明
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　山村　新也
福岡県福岡市早良区百道浜２丁目２番１号　富士通西日本コミュニケーション・システムズ株式会社内
(74)代理人　100077517
弁理士　石田　敬　（外４名）

最終頁に続く

(54)【発明の名称】　モバイルＩＰネットワークにおけるＶＰＮシステム及びＶＰＮの設定方法

(57)【要約】
【課題】　モバイルＩＰにおける位置登録手順と連携してＶＰＮ用の特殊な機能を持たせること無く、任意の端末間でのＩＰＳｅｃトンネルによるＶＰＮ設定サービスを提供する。
【解決手段】　移動端末と、認証サーバと、ＶＰＮデータベースと、ネットワーク装置とで構成され、ホーム認証サーバは、移動端末からの位置登録要求時に認証を要求したユーザのＶＰＮ情報をＶＰＮデータベースから抽出し、そのＶＰＮ情報を所定の位置登録メッセージ及び認証応答メッセージを用いて各ネットワーク装置に通知する。ネットワーク装置は、通知されたＶＰＮ情報を基にホームネットワーク装置と外部ネットワーク装置間、ホームネットワーク装置と所定のネットワーク装置間、及び／又は外部ネットワーク装置と所定のネットワーク装置間にそれぞれＩＰＳｅｃによるＶＰＮパスを設定する。

図２　本発明によるネットワーク構成の一例



【特許請求の範囲】

【請求項１】　ＩＰネットワーク上で端末がネットワーク間を移動したときに、ＩＰアドレスの管理と移動先への通信パケットの転送を自動化したプロトコルを用いたネットワークのホームネットワークに設けられるサーバ装置において、

前記端末と関連つけて、ＩＰネットワーク内に安全な通信路を構築するための情報を記憶する記憶手段と、

移動先の外部ネットワーク内の前記端末と、前記端末と通信を行う相手先端末との間に安全な通信路を構築できるように前記情報を分配する分配手段とを設けたことを特徴とするサーバ装置。

【請求項２】　前記分配手段は、相手先端末のある外部ネットワークのルータへ前記情報を転送することを特徴とする請求項１に記載のサーバ装置。

【請求項３】　前記安全な通信経路は仮想プライベート・ネットワークで実現される通信路であり、前記情報は前記仮想プライベート・ネットワークとしての設定経路情報とセキュリティ情報を含む情報であることを特徴とする請求項１に記載のサーバ装置。

【請求項４】　前記分配手段は、前記端末からの位置登録要求メッセージに対する認証応答メッセージ送出時に、前記情報を分配することを特徴とする請求項１に記載のサーバ装置。

【請求項５】　前記分配手段は、通信先となる相手先端末からの通信パケットを受け取った後に、前記情報を分配することを特徴とする請求項１に記載のサーバ装置。

【請求項６】　モバイルＩＰネットワークにおけるＶＰＮシステムは、

移動端末と、

ユーザのホームネットワークに設けられたホーム認証サーバとそれ以外の外部ネットワークに設けられた外部認証サーバと、

ホームネットワークに設けられたＶＰＮデータベースと、

ホームネットワーク、外部ネットワーク、及び所定の通信ホスト及び／又はその代理サーバの各ゲートウェイ機能を有するネットワーク装置と、

で構成され、

ホーム認証サーバは、移動端末からの位置登録要求時に認証を要求したユーザのＶＰＮ情報をＶＰＮデータベースから抽出し、そのＶＰＮ情報を所定の位置登録メッセージ及び認証応答メッセージを用いて各ネットワーク装置に通知し、

各ネットワーク装置は、通知されたＶＰＮ情報を基にホームネットワーク装置と外部ネットワーク装置間、ホームネットワーク装置と所定のネットワーク装置間、及び／又は外部ネットワーク装置と所定のネットワーク装置間にそれぞれＩＰＳｅｃによるＶＰＮパスを設定する、

ことを特徴とするＶＰＮシステム。

【請求項７】　認証サーバ及びネットワーク装置は、移動端末の移動による位置登録要求と連動して認証サーバ及びネットワーク装置にキャッシュされたＶＰＮ情報を新経路情報に更新するか、又はモバイルＩＰで通知される位置情報で書き換えることにより、ホームネットワーク装置と外部ネットワーク装置間、ホームネットワーク装置と所定のネットワーク装置間、及び／又は外部ネットワーク装置と所定のネットワーク装置間の各ＶＰＮパスを新たなＩＰＳｅｃによるＶＰＮパスに自動更新する、請求項６記載のシステム。

【請求項８】　ホーム認証サーバは、

前記ＶＰＮデータベースのＶＰＮ情報と、自身が保有すると通信先ホストを収容する所定のネットワーク装置との対応表を用い、所定の認証要求メッセージに設定された移動端末が接続した外部ネットワーク装置の情報と移動端末のホームネットワーク装置の情報からＶＰＮ設定経路を特定するＡＡＡＶＰＮ制御部と、

各ネットワーク装置間のサービス品質とセキュリティ情報をサービスプロファイルとして、アクセスネットワークへの所定の認証応答メッセージ及びホームネットワークへの位置登録メッセージに設定するＡＡＡプロトコル処理部と、

を有する請求項６記載の装置。

【請求項９】　各ネットワーク装置は、

キャッシュによりＶＰＮ情報が設定されたサービスプロファイルに関連するプロトコル群を制御するＭＡプロトコル処理部と、

そのサービスプロファイルに従ってサービス品質を保証するＱｏＳ制御とセキュリティゲートウェイ間のセキュリティを保証するためのトンネルを設定するＭＡＶＰＮ制御部と、

を有する請求項６記載の装置。

【請求項１０】　モバイルＩＰネットワークにおけるＶＰＮの設定方法は、

－　ユーザの移動端末から外部エージェントに位置登録要求メッセージを送信すること、

－　外部エージェントは受信した位置登録要求情報を含む認証要求メッセージを、自身のローカル認証サーバを介してユーザのホーム認証サーバへ送信すること、

－　ホーム認証サーバは、受信した認証要求メッセージより自身のデータベースを参照して通信先ホスト、ネットワーク装置種別、及びユーザ別のセキュリティ・サービス情報を抽出し、ネットワーク装置種別がＶＰＮ動的設定可である場合はＶＰＮキャッシュに外部エージェント－通信先ネットワーク装置のＶＰＮを設定して、それらの情報を含む位置登録要求メッセージをホームエージェントに送信すること、

－　ホームエージェントは、受信した位置登録要求メッセージをキャッシュし、位置登録処理の終了後にネットワーク装置種別がＶＰＮ動的設定可である場合は通信先

ホスト宛にこのＶＰＮ情報を付加した結合更新メッセージを送出すること、

－　ネットワーク装置は結合更新メッセージを代理受信し、それに付加されたＶＰＮ情報をキャッシュし、指定されたセキュリティ・サービスを設定し、ネットワーク装置から外部エージェントに向けたＩＰＳｅｃトンネルによるＶＰＮパスを設定し、その後に結合承認メッセージをホームエージェントに送信すること、

－　ホームエージェントは、結合承認メッセージを受信すると、位置登録応答メッセージをホーム認証サーバへ送信すること、

－　ホーム認証サーバは、位置登録応答メッセージの受信により、キャッシュしてある外部エージェント－ネットワーク装置間のＶＰＮ情報を付加した認証応答メッセージを外部エージェントのローカル認証サーバに送信すること、

－　ローカル認証サーバは、受信した認証応答メッセージをその付加されたＶＰＮ情報をキャッシュしてから外部エージェントへ送信すること、

－　外部エージェントは、受信した認証応答メッセージに含まれるＶＰＮ情報をキャッシュし、指定されたセキュリティ・サービスを設定し、外部エージェントからネットワーク装置に向けたＩＰＳｅｃトンネルによるＶＰＮパスを設定した後、ユーザの移動端末へ位置登録応答メッセージを返送すること、

から成ることを特徴とするＶＰＮの設定方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】近年インターネットの普及に伴い、企業の専用線をインターネット上の仮想パス（ＶＰＮ：Virtual Private Network）で置き換える事により、通信コストを低減しようとする試みが広く行われるようになってきている。また、電子商取引を実現する上でもインターネット上のセキュリティ強化は必須であり、これらを実現する技術としてＩＰ　Ｓｅｃｕｒｉｔｙ　Ｐｒｏｔｏｃｏｌ（以降、「ＩＰＳｅｃ」と称す）が注目されている。

【０００２】一方、ＩＭＴ－２０００の本格導入をきじかに控え、インターネット環境はモバイル環境への移行が始まっている。モバイル環境をインターネットへ導入することはそれを利用するユーザの利便性を高める。しかしながら、その一方でセキュリティを脆弱にする危険性も増大させることになり、モバイル環境でセキュリティを保護する枠組みが求められている。

【０００３】ＩＭＴ－２０００でコアネットワークアーキテクチャの基礎となるＲＦＣ２００２で規定された　ＩＰ　Ｍｏｂｉｌｉｔｙ　Ｓｕｐｐｏｒｔ（以降、「モバイルＩＰ（Mobile IP）」と称す）にＩＰＳｅｃを組み合わせる方式についても、いくつかの提案がされている。ここで、モバイルＩＰ（mobile internet protocol）とは、ＩＰネットワーク上で端末がネットワーク間を移動した時に、ＩＰアドレスの管理と移動先への通信パケットの転送を自動化した技術である。ルータにアドレスの転送を実行するエージェント機能を実装し、端末の"本籍"にあたるホーム・アドレスと現住所の"気付アドレス"の２つを管理させる。端末は、ネットワーク間を移動した際に新しい気付アドレスを、ホーム・アドレスのあるネットワークのルータに登録し、移動を知らない通信相手からのメッセージをトンネリング技術で転送させる。

【０００４】しかしこれらの提案は、通信経路上（具体的にはホームエージェントと通信端末との間）の完全なセキュリティを保証していないために、エンドユーザ端末がＩＰＳｅｃ機能を持つことを前提としている。これらの提案では、結局通信に関与する端末が全てＩＰＳｅｃを実装する必要があり、モバイル環境でセキュリティを保護する枠組みとしては、不十分であり、モバイルＩＰとＩＰＳｅｃとを連携させる意義が薄い。

【０００５】

【従来の技術】図１は、既存の提案によるモバイルＩＰ＋ＩＰＳｅｃを適用したネットワーク構成の一例を示したものである。ここでは、モバイル環境をサポートするＩＰアーキテクチャとしてＲＦＣ２００２で提案されたモバイルＩＰと、インターネット上でセキュリティを実現するアーキテクチャであるＩＰＳｅｃとを併用している。モバイルＩＰは、その本質から通常のネットワークに比較してセキュリティ面が脆弱なため、ＩＰＳｅｃを含む様々なセキュリティ強化の方式がとりいれられている。

【０００６】図１の例では、モバイルＩＰで規定されるユーザ１（ＭＮ：Mobile Node）がアクセスしたネットワーク２にある移動性エージェント２１（外部エージェントＦＡ：Foreign Agent）とユーザのホームネットワーク３にある移動性エージェント３１（ホームエージェントＨＡ：Home Agent）との間におけるＩＰ－ＩＰトンネルをＩＰＳｅｃトンネル６で置き換えるものであり、ＩＰＳｅｃで用いるＶＰＮ用の情報はあらかじめ各移動性エージェント２１及び３１に設定しておく必要がある。

【０００７】動的にＩＰＳｅｃトンネル７を設定することについてもこれらの提案で触れているが、移動端末１と移動性エージェント２１、３１との間の自動鍵交換（ＩＫＥ）に頼った方式であり、通信先ホスト５２（ＣＮ：Corespondent Node）とも自動鍵交換（ＩＫＥ）を用いて個別にＩＰＳｅｃを設定する必要がある。この場合、さらにモバイルＩＰの変更も必要となる。

【０００８】一般に、ＶＰＮはＩＰＳｅｃやＭＰＬＳ等を用いてインターネット上に張られるユーザの仮想パスのことを言うが、他のインターネット技術、例えばＤｉｆｆｅｒｅｎｔｉａｔｅｄ　Ｓｅｒｖｉｃｅ（以降、「差別化サービス」と称す）等、とユーザ単位では連携

しておらず、その結果ＶＰＮのサービス品質保証は十分なネットワーク資源の割当てと一貫な優先制御（例えば、ＩＰＳｅｃプロトコルのプロトコル番号をフィルタリング条件とした簡単な優先度制御）とによって行われている。

【０００９】

【発明が解決しようとする課題】上記で述べたような方式によれば、結局は通信に関与する端末が全てＩＰＳｅｃを実装する必要がある。そのため、ネットワークとしてＩＰＳｅｃサービスを提供する意義が薄く、またセキュリティサービスとサービス品質保証とを自由に組み合わせてユーザの利便性を向上させたネットワークサービスを、ＩＰＳｅｃを実装していない既存の端末を含めて、提供することが出来ないという問題があった。

【００１０】本発明の目的は、モバイルＩＰにおける通信を安全な通信経路を用いて可能にすることにある。また、本発明の目的は、モバイルＩＰにおける位置登録手順と連携して、通信に関与する端末の公衆ＩＰネットワークへのセキュリティゲートウェイに動的にＩＰＳｅｃを用いたＶＰＮを設定することによって、移動端末や通信端末にＶＰＮ用の特殊な機能を持たせること無く任意の端末間での通信にＶＰＮ設定サービスを提供し、ユーザの利便性向上させたＶＰＮサービスを提供することにある。それにより、ＶＰＮサービスを提供するサービスプロバイダの差別化も可能になる。

【００１１】より具体的には、以下のことを目的とする。

１）モバイルＩＰにおける位置登録手順と連携して、通信に関与する端末の公衆ＩＰネットワークへのセキュリティゲートウェイ２１、３１に動的にＩＰＳｅｃを用いたＶＰＮを設定することで、ＭＮ１やＣＮ４２、５２にＶＰＮ用の特殊な機能を持たせること無く、任意の端末間でのＶＰＮ設定サービスの提供を可能にする。

２）ユーザが自由に組み合わせて指定したサービス品質、セキュリティレベル、経路でのＶＰＮ設定を可能にする。

３）ＭＮ１の移動に伴い、ＶＰＮの経路を自動更新することを可能にする。

【００１２】

【課題を解決するための手段】図２には、図１の構成と対比させた本発明に基くネットワーク構成例を示しており、モバイルＩＰにおける位置登録手順と連携して、通信に関与する端末の公衆ＩＰネットワーク２～５の各セキュリティゲートウェイ２１～５１に動的にＩＰＳｅｃを用いたＶＰＮを設定することで任意の端末１やホスト３２～５２間の通信にＶＰＮ設定サービスを提供する。

【００１３】図３は、本発明の基本的な機能ブロック構成例を示したものである。最初に、以降で使用される用語の簡単な説明を行なっておく。ＭＩＰ（MobileIP）は、ＲＦＣ２００２と将来の全ての拡張で規定されるモバイルＩＰプロトコルである。ＡＡＡプロトコルは、ＡＡＡシステムが使用するプロトコルであって、本願の実施例では現在ＩＥＴＦで検討中のＤＩＡＭＥＴＥＲプロトコルの使用を想定している。ＡＡＡプロトコルは認証(Authentication)、認可(Authorization)、課金(Acounting)、及びポリシーに関する情報を伝達可能なあらゆるプロトコルで実装可能である。本発明で必要となる新たな情報の伝送には前記ＤＩＡＭＥＴＥＲプロトコルで定義されるＡＶＰ（Attribute Value Pair）と呼ばれる拡張可能な属性パラメータを用いる。拡張される属性はＶＰＮ設定に関する情報である。

【００１４】ＭＮ（Mobile Node）は、モバイルＩＰプロトコル機能を有する移動端末を示す。ＡＡＡは、上述した認証、認可、課金を行うサーバ群のＩＥＴＦで用いられる名称である。ＡＡＡＨは認証要求ユーザーの加入者データを持つネットワークのＡＡＡであり、ＡＡＡＦは該ユーザーの加入者データを持たないネットワークのＡＡＡである。本発明のＡＡＡは上記機能に加えてＶＰＮデータベースから認証要求ユーザのＶＰＮ情報を抽出し、ＨＡへＨＡ登録要求メッセージで、またＦＡへはＡＡＡＦを経由した認証応答メッセージでＶＰＮ情報を通知し、さらにユーザ単位のＶＰＮ情報の抽出とＶＰＮ経路の決定を行う。

【００１５】ＦＡ（Foreign Agent）は、ＲＦＣ２００２で定義される機能エンティティであって移動端末に割り付けられるホームアドレスを所有しないエージェントである。自ノードのアドレスである気付アドレス（Care-of-Address）にカプセル化されて送られてきたパケットをデカプセル化し、ホームアドレスに対応したリンクレイヤアドレスへ回送する。このアドレスの対応は、訪問者リストと呼ばれるテーブルで管理される。本発明のＦＡはＩＰＳｅｃのセキュリティゲートウェイ機能と差別化サービスのエッジルータ機能とを兼ね備える。

【００１６】ＨＡ（Home Agent）は、ＲＦＣ２００２で定義される機能エンティティであって移動端末に割り付けられたホームアドレスを所有するエージェントである。ＨＡに回送されてきた移動端末のホームアドレスを送信先とするパケットはホームアドレスに対応したＦＡの気付アドレスへカプセル化されて送出される。このアドレスの対応は移動結合と呼ばれるテーブルで管理される。本発明のＨＡはＩＰＳｅｃのセキュリティゲートウェイ機能と差別化サービスのエッジルータ機能を兼ね備える。

【００１７】ＰＣＮ（Proxy Correspondent Node）は、特許２０００－３２３７２号で規定された機能エンティティであって配下のモバイルＩＰをサポートしない通信ノード（ＣＮ；Correspondent Node）に代わって、ＨＡから送られてきたＣＮへの結合更新メッセージを代理受信し、結合更新で通知された宛先へ結合トンネルを設定する。本発明のＰＣＮはＩＰＳｅｃのセキュリティゲー

トウェイ機能と差別化サービスのエッジルータ機能を兼ね備えており．ＭｉＰプロトコルで通知されるＶＰＮ情報を解析し、その解析したＶＰＮ情報に基づいてネットワークカーネルに差別化サービスの設定と指定されたセキュリティレベルでのトンネルを設定する。

【００１８】本発明によれば、モバイル環境をサポートするＩＰネットワークは．ユーザ認証サーバ及びネットワーク装置で構成され、移動端末１からの初回位置登録要求（認証要求）時に、認証サーバ（ＡＡＡＨ）が認証を要求したユーザのＶＰＮ情報をＶＰＮデータベースから抽出し、そのＶＰＮ情報を位置登録メッセージ及び認証応答メッセージを用いてネットワーク装置（ＨＡ，ＦＡ）に通知する。ネットワーク装置（ＨＡ，ＦＡ）は、通知されたＶＰＮ情報を基にＨＡとＦＡ間にＶＰＮを設定する。その際．ネットワーク装置（ＨＡ）は．通信先端末ＣＮが他のネットワーク４に存在する場合は更にＨＡからＶＰＮ情報で指定された通信先端末収容のセキュリティゲートウェイ（ＰＣＮ）へＶＰＮを設定する。

【００１９】また、前記認証サーバ及びネットワーク装置は．移動端末１の移動による位置登録要求と連動して認証サーバ及びネットワーク装置にキャッシュされたＶＰＮ情報を新経路情報に更新するか又はモバイルＩＰで通知される位置情報で書き換える。その結果、新ＦＡとＨＡ間及びＰＣＮと新ＦＡ間に新たなＩＰＳｅｃトンネルが動的に設定され、ＶＰＮ経路が自動更新される。さらに．ＦＡ間のデータパケット転送におけるセキュリティ保護を完全なものとするため、スムースハンドオフ時のＦＡ間の結合トンネルにもＩＰＳｅｃトンネルが設定される。

【００２０】本発明の認証サーバ（ＡＡＡＨ）は．ユーザが所望するサービス品質．セキュリティゲートウェイ間のセキュリティ情報、及びＶＰＮを設定する通信先ホスト（ＣＮ）のＩＰアドレス群からなるユーザ単位のＶＰＮ情報と通信先ホストを収容するセキュリティゲートウェイ（ＶＰＮＧＷ）との対応表を格納するＶＰＮデータベースと、認証要求メッセージに設定された移動端末が接続したアクセスネットワーク２のセキュリティゲートウェイ（ＦＡ）アドレスと移動端末のホームネットワーク３のセキュリティゲートウェイ（ＨＡ）アドレス、及び前記ユーザ対応ＶＰＮ情報に設定された通信先ホスト（ＣＮ）と前記対応表から抽出される通信先ホストを収容するセキュリティゲートウェイ（ＰＣＮ；Proxy CN）アドレスからＶＰＮ設定経路を特定するＡＡＡＶＰＮ制御部と、各セキュリティゲートウェイ間のサービス品質とセキュリティ情報をサービスプロファイルとして．アクセスネットワークへの認証応答メッセージ及びホームネットワークへの位置登録メッセージに設定するＡＡＡプロトコル処理部と．を有する。

【００２１】また本発明のセキュリティゲートウェイから成るネットワーク装置（ＨＡ、ＦＡ．ＰＣＮ）は、上記ＶＰＮ情報を設定されたサービスプロファイルとＲＦＣ２００２とそれに関連するその他の拡張プロトコルを理解するためのＭＡ(Mobility Agent)プロトコル処理部と．通知されたサービスプロファイルに従いサービス品質を保証するＱｏＳ制御とセキュリティゲートウェイ間のセキュリティを保証するためのトンネルを設定するＭＡＶＰＮ制御部と、を有する。

【００２２】前記ＭＡプロトコル処理部は、配下のモバイルＩＰをサポートしないＣＮに代わってＨＡからのＣＮへの結合更新メッセージを代理受信し、結合更新で通知されたＶＰＮ情報が設定されたサービスプロファイルを基に、ＣＮに代わってＦＡへの結合トンネルをＩＰＳｅｃトンネルで設定するプロトコル処理を行なう。

【００２３】移動端末（ＭＮ）１のホームネットワーク３にあるネットワーク装置（ＨＡ）のＭＡＶＰＮ制御部は．前記トンネルの設定の際にサービスプロファイルでセキュリティ保護が要求されるとＲＦＣ２００２で規定されたＨＡから移動端末の現在の接続点である外部ネットワーク２にあるネットワーク装置（ＦＡ）に設定するトンネルを通常のＩＰ－ＩＰトンネルに代わりＩＰＳｅｃトンネルを設定し、一方ＦＡの側のＭＡＶＰＮ制御部もサービスプロファイルでセキュリティ保護が要求されると．ＦＡからＨＡへのトンネル（通常リバーストンネルと呼ばれる）をＩＰ－ＩＰトンネルではなくＩＰＳｅｃトンネルで設定する。

【００２４】上述したように、本発明によればモバイルＩＰにおける位置登録手順と連携して．通信に関与する端末の公衆ＩＰネットワークへのセキュリティゲートウェイに動的にＩＰＳｅｃを用いたＶＰＮが設定される。従って、移動端末（ＭＮ）や通信先ホスト（ＣＮ）にＶＰＮ用の特殊な機能を待たせること無く任意の端末やホスト間でＶＰＮ設定サービスが提供可能となる。また、ネットワーク側でＶＰＮ設定サービスが提供されるため．ユーザによる自由な組み合わせによるサービス品質．セキュリティレベル．及び経路等の指定が可能となる。

【００２５】

【発明の実施の形態】図４は、本発明の第１の実施例を示したものである。本例は．初期位置登録時のＶＰＮ設定例（静的ＨＡ－ＣＮ間ＶＰＮ存在時）を示しており、あるユーザがＶＰＮサービスを提供しているＩＳＰ(Internet Service Provider) を利用して自分が勤めている企業に公衆ネットワークからアクセスする時に．自動的にＶＰＮが設定されるような契約をした場合を想定している。以降では．本願発明の理解の容易のため．本実施例の説明と併せて図３で示した本発明の各機能ブロックのより詳細な構成及び動作について随時説明していく。

【００２６】図４において．上記サービスを望むユーザ１は．まず企業５とホームＩＳＰ３との間でＶＰＮ契約（ＳＬＡ：Service Level Agreement ）を取り交わす

（①）。契約内容は使用するＳＰＩ（Security Parameter Index）と鍵群、サービス品質、このＶＰＮを利用可能なユーザのリストである。企業側は前記ＳＬＡに基づき、自企業のＶＰＮＧＷ装置５１にＩＳＰ３のＨＡ３１のＶＰＮ情報を設定する。ＩＳＰ側は企業に示されたユーザのＶＰＮデータベースにこの企業ドメインのアドレスとＳＰＩ、鍵等を設定する。またＶＰＮ情報３５としてＣＮ－ＧＷ対応表に企業ドメインアドレスとＶＰＮＧＷ装置５１のアドレスを登録し、ＧＷ種別にＶＰＮ動的設定不可を設定する。

【００２７】図５には、本発明で使用するＶＰＮデータベースの構成例を示している。ＶＰＮデータベース３４は各ユーザの設定したＶＰＮデータインスタンス１～ｎの集合であり、各インスタンスが一つのＶＰＮに対応する。各ＶＰＮデータインスタンスは、このＶＰＮ情報を一意に表す識別子であるプロファイル番号（Profile Number）、ユーザのネットワーク識別子（ＮＡＩ；Network Access Identifier）、セキュリティゲートウェイ間の共有のセキュリティ関係を使用するか又はユーザ固有のセキュリティ関係を使用するかを示すＶＰＮ共有指標（vpnshare）、通信先端末のＩＰアドレス（destaddr）、上り方向のＱｏＳクラス（upclass）、下り方向のＱｏＳクラス（downclass）、ＩＰＳｅｃで使用する上り方向ＳＰＩ（upSPI）、ＩＰＳｅｃで使用する下り方向ＳＰＩ（downSPI）で構成される。

【００２８】前記ＶＰＮ共有指標にＯが設定された場合、ｕｐｃｌａｓｓ，ｄｏｗｎｃｌａｓｓ，ｕｐＳＰＩ，ｄｏｗｎＳＰＩは省略可能である。このデータベースはユーザのＮＡＩで検索され、検索された全てのインスタンスは後述するＶＰＮ情報キャッシュにアドレス情報を付加して記録される。なお、データ検索に使用するデータベース検索プロトコルはＶＰＮデータベースを実装するデータベースの製品等に依存しており、通常はＬＤＡＰ（Light Directory Access Protocol）やＳＱＬが用いられる。また、上述したＶＰＮ情報３５のＣＮ－ＧＷ対応表については後述の図８にその一例を示す。

【００２９】次に、ユーザ１は企業が契約を交わしたホームＩＳＰ３とローミング契約をしているＩＳＰ２の任意のアクセスポイントに接続し、モバイルＩＰの位置登録要求（Ｒｅｇ　Ｒｅｑ）（②）を送出することでネットワークの利用が可能になる。ローミング契約しているＩＳＰ２の接続ポイントとなるＦＡ２１はこの登録要求を認証要求メッセージ（ＡＭＲ）（③）に含めて、自ＩＳＰ内のローカルＡＡＡサーバ（ＡＡＡＦ）２３を介して、ユーザのホームＩＳＰ３のＡＡＡ（ＡＡＡＨ）３３に送出する。

【００３０】ＡＡＡＨは認証要求メッセージ（ＡＭＲ）に含まれるＮＡＩでＶＰＮデータベース３４を検索し、このユーザに固有のＶＰＮ情報３５を抽出する。また、そのＣＮ－ＧＷアドレス対応表よりＶＰＮデータベースで通信先として指定されている企業ドメインのアドレスはＶＰＮ動的設定不可であることがわかるので、後述するＶＰＮ情報キャッシュにＦＡ－ＨＡ、ＨＡ－企業ＧＷの２つのＶＰＮを設定する。次に、ＨＡに対してこの２つのＶＰＮのプロファイルを付加した位置登録要求メッセージ（ＨＡＲ）を送信する（④）。

【００３１】図６にはＡＡＡの詳細機能ブロックを、そして図７～１２にはその動作例を示している。図６において、ＡＡＡ３３（２３も同様）は、図３で示したＡＡＡプロトコル制御部３０１、ＡＡＡＶＰＮ制御部３０２に加えて、アプリケーションサーバ３０５、ネットワークカーネル３０３、及び物理ネットワークデバイスインタフェース３０４から構成される。ＡＡＡプロトコル制御部３０２は、ＡＡＡプロトコルを制御するＡＡＡプロトコル処理部３１１から構成される。

【００３２】ＡＡＡＶＰＮ制御部３０２は、ＶＰＮデータベース（図５）より抽出したＶＰＮ情報をキャッシュするＶＰＮ情報キャッシュ３１２、ＶＰＮ経路決定制御部３１３、鍵生成器３１５から構成される。図７には、ＶＰＮ情報キャッシュ３１２の一例を示している。ＶＰＮ情報キャッシュ３１２はＶＰＮ情報キャッシュインスタンス１～ｎの集まりであり、ユーザがネットワークにアクセスしている間有効なネットワークで一意なユーザに固有な情報を含むセッションＩＤで検索される。各ＶＰＮ情報キャッシュインスタンス１～ｎは一意な識別子であるセッションＩＤ、このユーザが設定しているＶＰＮの数を示すプロファイル数、各ＶＰＮの設定情報を含むＶＰＮ情報プロファイル１～ｎで構成される。

【００３３】各ＶＰＮ情報プロファイル１～ｎは、ＶＰＮを一意に識別する識別子であるプロファイル番号、ＶＰＮ適用のパケットを特定するための送信元と宛先のＩＰアドレストとそのネットマスク、パケットに設定するＴＯＳ値、ＩＰＳｅｃをＡＨ，ＥＳＰ，カプセル化のみ、のいずれかで設定するかを示すセキュリティタイプ、ＩＰＳｅｃトンネルモードで参照されるＩＰＳｅｃトンネルの入口と出口である送信元と宛先のゲートウェイアドレス、宛先ゲートウェイが動的なＶＰＮ設定が可能かどうかを示す宛先ＧＷ種別、上りと下り方向のセキュリティ関係の識別子であるＳＰＩ（Security Parameter Index）、ＥＳＰ暗号鍵，ＥＳＰ認証鍵で構成される。

【００３４】ＶＰＮ経路決定制御部３１３は、その内部にＣＮ－ＧＷアドレス対応表３１４を有しており、図８にＣＮ－ＧＷアドレス対応表の一例を示している。ＣＮ－ＧＷアドレス対応表は、ＣＮアドレス／ネットマスク，ＧＷアドレス、及びＧＷ種別を含むアドレスインスタンス１～ｎから構成され、ＣＮアドレス／ネットマスク（企業ドメインアドレス）をキーとして検索される。

【００３５】アプリケーションサーバは、ＶＰＮデータベース３４とＷＥＢアプリケーション３６から構成され

る。ネットワークカーネル３０３はＩＰパケットの回送とネットワークへの接続点である物理インタフェースを制御するオペレーティングシステムである。物理ネットワークデバイスインタフェース３０４は物理ネットワークデバイスへのインタフェース（ハード制御ドライバ）であり、通常はＬＡＮのＮＩＣカードである。

【００３６】図９～１３は、ＡＡＡの処理フローの一例を示している。図９はＡＡＡの全体処理フロー例であって、ネットワークカーネル３０３が物理ネットワークインタフェース３０４からパケットを受信すると、そのポート番号によりＡＡＡシグナリングパケットを選択し、ＡＡＡプロトコル制御部３０１に受信パケットの情報を渡す（Ｓ１００）。図１０はＡＡＡプロトコル処理部３１１の処理フロー例である。先ず、受信したＡＡＡプロトコルのコマンドコードＡＶＰ（属性パラメータ）より受信メッセージを判定する（Ｓ１０１）。認証要求メッセージ（ＡＭＲ）であればステップＳ１０２へ、後述する認証応答メッセージ（ＡＭＡ）であればステップＳ１０３へ、その他であればステップＳ１０４へ処理を分岐する。

【００３７】上記した本例の場合には、ＡＡＡＶＰＮ制御部３０２を起動する（Ｓ１０２）。次に、ＶＰＮデータベース３４より抽出したＶＰＮ情報又は認証応答メッセージ（ＡＭＡ）をＶＰＮ情報キャッシュに設定する（Ｓ１０３）。そして、ＣＮ－ＧＷ対応表に従って対応メッセージを編集、例えば、差別化サービスの設定等をしてから送出する（Ｓ１０４）。ＡＡＡＨ３３が送出する認証応答メッセージ（ＡＭＡ）及び位置登録要求メッセージ（ＨＡＲ）にはＶＰＮ情報キャッシュを設定した旨のプロファイルキャッシュＡＶＰ(Profile Cache AVP) を設定する。なお、図１１には、図１０のステップＳ１０３におけるメッセージ対応表（送受信メッセージとその処理実行主体との関係）を示している。

【００３８】図１２は、ＡＡＡＶＰＮ制御部３０２の処理フロー例である。ＡＡＡＶＰＮ制御部３０２は、始めにＶＰＮデータベース３４を移動端末のＮＡＩで検索して対応するＶＰＮ情報を読み出す（Ｓ１０５）。次にＶＰＮ経路決定制御部３１３を起動し（Ｓ１０６）、そしてＶＰＮデータベース３４から読み出したＳＰＩ（Security Parameter Index）がデフォルトＳＰＩであれば処理を終了し、そうでなければ鍵生成器３１５で個別の鍵を生成する（Ｓ１０８）。

【００３９】図１３は、ＶＰＮ経路決定制御部３１３の処理フロー例である。ＶＰＮ経路決定制御部３１３は、認証要求メッセージ（ＡＭＲ）の要求元ホストアドレスからＭＮ１側のＶＰＮＧＷ（ＦＡ）２１のアドレスを抽出する（Ｓ１０９）。また、ＶＰＮデータベース３４から読み出したＣＮアドレスによりＣＮ－ＧＷアドレス対応表３１４を検索してＣＮ５２側のＶＰＮＧＷ５１のアドレスとＶＰＮＧＷ種別を読み出す（Ｓ１１０）。

【００４０】次に、前記ＶＰＮＧＷ種別が動的ＶＰＮ設定可能であればステップＳ１１２へ、そうでなければステップＳ１１３へ処理を分岐する（Ｓ１１１）。本例ではステップＳ１１３の処理を行なうことになる。この場合、ＨＡ３１へ通知するＶＰＮ情報の送信元ＧＷアドレスにＨＡ３１のアドレス、宛先ＧＷアドレスにＣＮ－ＧＷアドレス対応表３１４から読み出したＧＷ５１のアドレスを設定する。また、ＦＡ２１へ通知するＶＰＮ情報の送信元ＧＷアドレスにＦＡ２１のアドレス、宛先ＧＷアドレスにＨＡ３１のアドレスを設定して処理を終了する（経路をＦＡ－ＨＡ－ＣＮに設定）。

【００４１】一方、ＶＰＮＧＷ種別が動的ＶＰＮ設定可能であれば、ＨＡ３１へ通知するＶＰＮ情報の宛先ＧＷアドレスにＦＡ２１のアドレス、送信元ＧＷアドレスにＣＮ－ＧＷアドレス対応表３１４から読み出したＧＷ５１のアドレスを設定する。ＦＡ２１へ通知するＶＰＮ情報の送信元ＧＷアドレスにＦＡ２１のアドレス、宛先ＧＷアドレスに同じくＣＮ－ＧＷアドレス対応表より読み出したＧＷ５１のアドレスを設定し終了する（経路をＦＡ－ＣＮ（又はＰＣＮ）に設定）。

【００４２】図４に戻って、次にＨＡ３１はＡＡＡＨ３３から受信した位置登録要求メッセージ（ＨＡＲ）に付加されたＶＰＮ情報をキャッシュし、さらに指定された差別化サービスのマッピングを行った後、受信した経路情報に従ってＨＡ３１から企業ＧＷ５１へのＩＰＳｅｃトンネル（２）とＨＡ３１からＦＡ２１へのＩＰＳｅｃトンネル（３）を設定する。また逆方向トンネルのパケットを復号するための情報を後述するＩＰＳｅｃ情報テーブルに設定する。なお、企業側のＧＷ５１からＨＡ３１へのＩＰＳｅｃトンネル（１）は最初の契約設定（ＳＬＡ）に基いて既に固定的に張られているため、ＨＡ３１から企業ＧＷ５１への設定処理は不要である。ＨＡ３１は位置登録処理終了後に位置登録応答メッセージ（ＨＡＡ）をＡＡＡＨ３３に返送する（⑮）。

【００４３】ＡＡＡＨ３３は前記位置登録応答メッセージ（ＨＡＡ）を受信すると、次にＶＰＮ情報キャッシュ３１２からＦＡ－ＨＡ間のＶＰＮを抽出し（図１３のＳ１１３参照）、ＦＡ２１に対して設定するこのＶＰＮのプロファイルを付加した認証応答メッセージ（ＡＭＡ）をＡＡＡＦ２３へ送信する（⑯）。ＡＡＡＦ２３はＭＮ１のローカルドメイン内での移動に対応するためＶＰＮ情報をＡＡＡＦ２３内にキャッシュした後にそれをＦＡ２１に回送する（図１０のＳ１０１、１０３、及び１０４参照）。

【００４４】ＦＡ２１は、認証応答メッセージ（ＡＭＡ）に付加されたＶＰＮ情報をキャッシュし、さらに指定された差別化サービスのマッピングを行った後に、ＦＡ２１からＨＡ３１へのＩＰＳｅｃトンネル（４）を設定する。また逆方向トンネルのパケットを復号するための情報をＩＰＳｅｃ情報テーブルに設定する。最後に、

登録応答メッセージ（Ｒｅｇ　Ｒｅｐ）をＭＮ１に返送する（⑰）。その結果、ＭＮ１のアクセスポイントから企業のＧＷ５１までのＶＰＮが設定される。なお、企業が指定していないユーザはＩＰＳｅｃトンネルを介してパケットが回送されないので、これを利用して不正ユーザのアクセスを防ぐことも可能になり、また複数のＩＳＰとＳＬＡを契約する煩わしさから逃れることができる。

【００４５】図１４にはＭＡ（ＦＡ、ＨＡ、ＰＣＮ）の詳細機能ブロックを、そして図１５～２４にはその動作例を示している。図１４において、ＦＡ、ＨＡ、ＰＣＮの各ネットワーク装置は、ＭＡプロトコル制御部３２１、ＭＡＶＰＮ制御部３２２、ネットワークカーネル３２３、及び物理ネットワークデバイスインタフェース３２４から構成される。ＭＡプロトコル制御部３２１は、ＡＡＡプロトコルを制御するＡＡＡプロトコル処理部３３１とモバイルＩＰを制御するモバイルｉＰプロトコル処理部３３２から構成される。また、ＭＡＶＰＮ制御部３２２は、ＡＡＡ又はＭＩＰプロトコルにより通知されたＶＰＮ情報をキャッシュするＶＰＮ情報キャッシュ３３３、ＱｏＳ制御部３３４、及びトンネル制御部３３５から構成される。

【００４６】ＶＰＮ情報キャッシュ３３３は先に図７で説明したのと同様の構成である。ＱｏＳ制御部３３４は、ＶＰＮ情報キャッシュ３３３に設定されたＴＯＳ値と、ＴＯＳ値をマーキングするパケットを識別するための送信元アドレス、宛先アドレス及びそれらのネットマスクからなるフィルタ情報をネットワークカーネル３２３に設定する。トンネル制御部３３５は、ＶＰＮ情報キャッシュ３３３に設定された宛先のＩＰアドレストに対してルートテーブル３３７の出口デバイスを仮想デバイスに書き換える。またｉＰＳｅｃ情報テーブル３３６に送信元と宛先のＩＰアドレストとそのネットマスク、セキュリティタイプ、送信元と宛先のゲートウェイアドレス、上りと下り方向のセキュリティ関係の識別子であるＳＰＩ、ＥＳＰ暗号鍵、ＥＳＰ認証鍵を設定する。ネットワークカーネル３２３から仮想デバイスに出力されたパケットはｉＰＳｅｃ情報テーブル３３５を参照して、暗号化とカプセル化が実行される。

【００４７】図１５には、ＩＰＳｅｃ情報テーブル３３３の一例を示している。ＩＰＳｅｃ情報テーブルは、ｉＰＳｅｃ情報、ＥＳＰ情報、トンネル情報で構成される。ＩＰＳｅｃ情報はｉＰＳｅｃ情報インスタンスの集まりであり、送信元アドレスと宛先アドレスの組で特定される。ｉＰＳｅｃ情報インスタンスは送信元アドレス／ネットマスク、宛先アドレス／ネットマスク、パケットの実際の回送先である実宛先アドレス、このパケットに適用するトンネル情報の識別子、このパケットに適用するＥＳＰ情報の識別子から構成される。ＥＳＰ情報はＥＳＰ情報インスタンスの集まりであり、ＥＳＰ情報を

一意に識別するＥＳＰ識別子、暗号化手法、方向、ＡＨ認証鍵長、ＥＳＰ認証鍵長、ＥＳＰ暗号鍵長、ＡＨ認証鍵、ＥＳＰ認証鍵、ＥＳＰ暗号鍵で構成される。トンネル情報はトンネル情報インスタンスの集まりであり、トンネル情報を一意に識別するトンネル識別子、カプセル化手法、方向、トンネルの入口と出口になる送信元アドレスと宛先アドレスから構成される。

【００４８】ネットワークカーネル３２３は、ＩＰパケットの回送とネットワークへの接続点である物理インタフェースを制御するオペレーティングシステムであり、ＩＰパケット回送のルートを決定するルーティングテーブル３３７を持つ。ネットワークカーネル３２３はＩＰパケットのカプセル化、パケット編集、パケット送出のキュー制御等を行うが、これらの機能はオペレーティングシステムに依存しており、本発明では言及しない。

【００４９】図１６にルーティングテーブル３３７の一例を示す。一般的なルーティングテーブル３３７は、宛先アドレス、ゲートウェイアドレス、ネットマスク、メトリック、出口インタフェースとその他の制御用補助情報から構成されており、宛先アドレスとメトリックでルートが決定される。本発明はルートテーブルの構成には依存しないが、出力先に仮想デバイスを設定できるようなネットワークカーネルを例に以降の具体的な説明を行う。又、ネットワークカーネルはカプセル化されたパケットを受信すると、パケットをデカプセル化する機能を持っており、デカプセル後のパケットがＥＳＰヘッダを含んでいれば、トンネル制御部３３５で保持しているＥＳＰ情報を参照して暗号化されたパケットをデコードする機能を持つ。物理ネットワークデバイスインタフェース３２４は物理ネットワークデバイスへのインタフェース（ハード制御ドライバ）であり、物理ネットワークデバイスは例えばＬＡＮ、ＩＳＤＮ、ＡＴＭ等のパッケージ又はＮＩＣカードである。

【００５０】図１７～２４には、ＭＡの処理フロー例を示している。以下、各処理フロー例を用いて本願発明によるＭＡ処理について説明する。図１７は、ＭＡの全体処理フローである。ネットワークカーネル３２３は物理ネットワークインタフェース３２４よりパケットを受信すると、既に概略を説明したようにデカプセル化及び暗号化復号を行った後、受信パケットをシグナリングパケットかデータパケットかで切り分ける（Ｓ２００）。シグナリングパケットの選択はＭＡプロトコル制御部３２１が指定したポート番号でパケットを受信したかどうかで決定される。シグナリングパケットであればステップＳ２０１、それ以外であればステップＳ２０３へ処理を分岐する。

【００５１】シグナリングパケットの場合はＭＡプロトコル制御部３２１へ受信パケットの情報を渡し、ＡＡＡプロトコル処理３３１及びモバイルＩＰプロトコル処理３３２を行う（Ｓ２０１）。次に、ＭＡＶＰＮ制御部３

２２を起動してＶＰＮ情報の設定を行う（Ｓ２０２）。ステップＳ２０３では、ネットワークカーネルが受信パケットの出力先のインタフェースを、ルーティングテーブル３３７を参照して決定する。ネットワークカーネル３２３はカーネル内に予め設定された差別化サービスのフィルタリング条件に従ってパケットの編集を行う。出力先が仮想デバイスであればステップＳ２０４へ処理を分岐する。出力先が物理デバイスであれば、そのデバイスへパケットを回送する。

【００５２】ステップＳ２０４では、ＭＡＶＰＮ制御部３２２へ回送するパケットの情報を渡し、予め設定された情報に基づきトンネル化及び暗号化処理を行う。トンネル処理でＩＰパケットをカプセル化する場合は、オリジナルパケットのＴＯＳ情報を引き継ぐ。ＩＰパケットの編集が終了したパケットは、再度、ネットワークカーネル３２３に戻され、新しく付与されたＩＰパケットの宛先に基づいてルーティングテーブル３３７が参照されて対応する物理デバイスへパケットの回送が行われる。

【００５３】図１８は、ＭＡプロトコル制御部３２１の処理フロー例である。先ず、受信したパケットのポート番号を調べ、ＡＡＡプロトコルのポート番号であればステップＳ２０６へ、一方モバイルＩＰプロトコルであればステップＳ２０７へ処理を分岐する（Ｓ２０５）。ステップＳ２０６では、ＡＡＡプロトコル処理部３３１を起動してＡＡＡプロトコルの処理後に（図１９参照）、ＡＡＡプロトコルに情報の一部として付加されているモバイルＩＰプロトコルを取り出してステップＳ２０７へ処理を渡す。ステップＳ２０７では、モバイルＩＰプロトコル処理部３３２を起動して処理を終了する。

【００５４】図１９は、ＡＡＡプロトコル処理部３３１の処理フロー例である。先ず、受信したＡＡＡプロトコルより、ＶＰＮ情報を抽出してそれをＶＰＮ情報キャッシュ３３３へ設定する。次に、後述のモバイルＩＰプロトコル処理部３３２が参照するために、キャッシュの設定及び更新を行った場合に共有メモリ上に更新したことを示すフラグを立てる（Ｓ２０８）。ＡＡＡプロトコルの処理後、ＡＡＡプロトコルに情報の一部として付加されているモバイルＩＰプロトコルを取り出す（Ｓ２０９）。そして、受信メッセージが位置登録要求メッセージ（ＨＡＲ）なら位置登録応答メッセージ（ＨＡＡ）を送出する（Ｓ２１０及び２１１）。

【００５５】図２０はモバイルＩＰプロトコル処理部３３２の処理フロー例である。ステップＳ２１２では、受信したモバイルＩＰプロトコルメッセージのタイプを判定する。タイプが登録要求であればステップＳ２１３へ、登録応答であればステップＳ２２０へ、ＢＵ(Binding Update)、ＢＡ(Binding Acknowledge)であばステップＳ２１８へそれぞれ処理を分岐する。

【００５６】Ａ．登録要求の場合

登録要求を受信したＭＡがＨＡの場合は、登録要求メッセージの気付アドレスと移動性結合内の旧気付アドレスとを比較し、比較結果が異なればステップＳ２１４へ処理を分岐する。比較結果が一致した場合又は登録要求を受信したＭＡがＦＡの場合はステップＳ２１７へ処理を分岐する（Ｓ２１３）。ステップＳ２１４では位置登録メッセージを送出したＭＮのＶＰＮ情報キャッシュインスタンスを特定し、ＶＰＮ情報キャッシュ３３３の宛先ＧＷアドレスを気付アドレスで通知されたアドレスに書き換える。

【００５７】この特定方法は例えばセッションＩＤにＭＮのＩＰアドレスを持たせることや、移動性結合とＶＰＮ情報キャッシュインスタンスのリンクを持たせることで実現可能である。ＨＡは特定したＶＰＮ情報キャッシュインスタンスに設定されている全てのＶＰＮ情報プロファイルを検索し、宛先ＧＷ種別が動的ＶＰＮ設定可能であれば、そのプロファイルの送信元アドレスに対してＶＰＮ情報を設定したＢＵメッセージを編集して送出する（Ｓ２１５）。ステップＳ２１６ではＭＡＶＰＮ制御部３２２を起動し、図２１のメッセージ対応表に示すように、受信メッセージと処理ＭＡで特定されるメッセージを編集して送出する（Ｓ２１７）。

【００５８】Ｂ．登録応答の場合

ステップＳ２２０では、ＡＡＡプロトコル処理部３３１によりあらかじめ共有メモリに設定されたキャッシュ更新情報を参照し、更新有りであればステップＳ２１６へ、更新無しであればステップＳ２１７へ処理を分岐する。

【００５９】Ｃ．ＢＵ，ＢＡの場合

ステップＳ２１８では、受信メッセージがＢＵであればステップＳ２１９へ、ＢＡであればステップＳ２１７へ処理を分岐する。ＰＣＮの場合は、ＰＣＮ配下のＣＮ宛てのＢＵメッセージを全て代理受信する。この仕組みは、例えば特許２０００－３２３７２の方式で実現される。処理ＭＡがＰＣＮの場合はＢＵメッセージに設定されたＶＰＮ情報をＶＰＮ情報キャッシュ３３３に設定もしくは置換する。処理ＭＡがＦＡの場合はＶＰＮ情報キャッシュ３３３の宛先ＧＷアドレスをＢＵメッセージで通知された新ＦＡアドレスに変更する（Ｓ２１９）。

【００６０】図２２は、ＭＡＶＰＮ制御部３２２の処理フロー例である。ステップＳ２２１ではＱｏＳ制御部３３４を起動し、次にステップＳ２２２でトンネル制御部３３５を起動する。図２３は、ＱｏＳ制御部３３４の処理フロー例である。先ず、ステップＳ２２３でＶＰＮ情報インスタンスの情報を元にネットワークカーネル３２３に設定済みの差別化サービスの情報を削除する。次に、ＶＰＮ情報インスタンスのＴＯＳ値が０以外であればステップＳ２２５へ処理を分岐し、そうでなければ処理を終了する（Ｓ２２４）。ステップＳ２２５では、ＶＰＮ情報インスタンスの情報を元にネットワークカーネルに差別化サービスの情報を設定する（Ｓ２２５）。

【００６１】図２４は、トンネル制御部の処理フロー例である。先ず、ＶＰＮ情報インスタンスの情報を元にネットワークカーネル３２３に設定済みのルートテーブル３３７の情報とＩＰＳｅｃ情報テーブル３３６の該当する情報を削除する（Ｓ２２６）。次に、ＶＰＮ情報インスタンスのＶＰＮ情報プロファイルに設定された宛先アドレスの出力先を仮想デバイスに設定し（Ｓ２２７）、またＶＰＮ情報インスタンスのＶＰＮ情報プロファイルを参照して、ＩＰＳｅｃ情報テーブル３３６のトンネル情報インスタンスを設定する（Ｓ２２８）。

【００６２】ステップＳ２２９では、ＶＰＮ情報インスタンスのＶＰＮ情報プロファイル内セキュリティタイプを参照して、ＥＳＰかＡＨが指定されていればステップＳ２３０へ処理を分岐し、そうでなければ処理を終了する。ステップＳ２３０では、ＶＰＮ情報インスタンスのＶＰＮ情報プロファイル内ＳＰＩを参照して、ＳＰＩがユーザ個別であればステップＳ２３１へ、デフォルトＳＰＩであればステップＳ２３２へ処理を分岐する。このデフォルトＳＰＩについては予めＭＡ内に初期構成時やＭＡのローカルな保守コンソールから設定されているものとする。ステップＳ２３１では、ＶＰＮ情報インスタンスのＶＰＮ情報プロファイルのＳＰＩと関連する鍵情報をＥＳＰ情報インスタンスに設定する。また、ステップＳ２３２では、ＩＰＳｅｃ情報インスタンスにＥＳＰ識別子を設定する。

【００６３】以降では、これまで説明してきた事項をもとに、本願発明動作の理解をより一層深めるために、先に説明した第１の実施例とは別の本発明の種々の実施態様例について説明する。図２５は、本発明の第２の実施例を示したものである。本例は、同一ドメイン内移動時のＶＰＮ設定例（静的ＨＡ－ＣＮ間ＶＰＮ存在時）を示している。ここでは、先の実施例１でローミング契約ＩＳＰ２のＦＡ２１から企業ドメインのＧＷ５１にＶＰＮが設定された後、ユーザのＭＮ１が同一ローミング契約ＩＳＰ２の別のＦＡ２１’に移動した場合に、どのようにＶＰＮが再構築されるかを図式的に示している。

【００６４】図２５において、ユーザのＭＮ１が同一ドメイン２内でＦＡ２１から新ＦＡ２１’へ移動すると、モバイルＩＰ経路最適化ドラフト（draft-ietf-mobileip-optim-09）に規定されているように、旧ＦＡ２１のアドレスを含めた登録要求メッセージ（Ｒｅｇ　Ｒｅｑ）を送出する（①）。新ＦＡ２１’はこの登録要求を認証要求メッセージ（ＡＭＲ）に含めて（②）、自ＩＳＰ２内のローカルＡＡＡサーバ（ＡＡＡＦ）２３に送出する。ＡＡＡＦ２３は、認証要求メッセージ（ＡＭＲ）に旧ＦＡ２１の情報が含まれている場合、ＶＰＮ情報キャッシュからＦＡ－ＨＡのＶＰＮを抽出してＦＡ２１のアドレスを新ＦＡ２１’のアドレスに置換した後、ＦＡに設定するこのＶＰＮのプロファイルを付加した認証応答メッセージ（ＡＭＡ）を新ＦＡ２１’へ返送する（③）。

【００６５】ＦＡ２１’は先にＭＮ１から受信した登録要求メッセージ（Ｒｅｇ　Ｒｅｑ）をＨＡ３１に回送する（④）。ＨＡ３１はＶＰＮ情報キャッシュのうち、ＨＡからＦＡへのＶＰＮプロファイルを特定し、ＦＡのアドレスを新ＦＡ２１’に書き換える。次に、旧ＦＡ２１へのＩＰＳｅｃトンネルを削除し、新ＦＡ２１’へ新たなＩＰＳｅｃトンネル（１）を設定する。そして、位置登録処理終了後、登録応答メッセージ（Ｒｅｇ　Ｒｅｐ）をＦＡ２１’に返送する（⑤）。

【００６６】ＦＡ２１’は、ＶＰＮ情報キャッシュを参照して指定された差別化サービスのマッピングを行った後、ＦＡ２１’からＨＡ３１へのＩＰＳｅｃトンネル（２）を設定する。また逆方向トンネルのパケットを復号するための情報をＩＰＳｅｃ情報テーブルに設定する。さらに、ＶＰＮ情報キャッシュを複写して送信元ＧＷアドレスを旧ＦＡ２１、宛先ＧＷアドレスを新ＦＡ２１’に書き換えた後に、このＶＰＮ情報をＢＵメッセージに付加して旧ＦＡ２１に送信する（⑥）。

【００６７】旧ＦＡ２１はＢＵメッセージに付加されたＶＰＮ情報をキャッシュし、ＦＡ２１からＨＡ３１へのＩＰＳｅｃトンネルを削除し、指定された差別化サービスのマッピングを行った後、旧ＦＡ２１から新ＦＡ２１’へスムースハンドオフ時のＩＰＳｅｃトンネル（３）を設定する。その結果、ＨＡ３１が新たなＩＰＳｅｃトンネル（１）への切り替え前にＭＮ１宛に旧ＦＡ２１で受信したパケットは全てこのＩＰＳｅｃトンネル（３）を介して新ＦＡ２１’へ回送される。旧ＦＡ２１はＩＰＳｅｃトンネル（３）の設定完了後にＢＡメッセージをＭＮに返送する（⑦）。これにより、新ＦＡ２１’は登録応答メッセージ（Ｒｅｇ　Ｒｅｐ）をＭＮ１に返送する（⑧）。

【００６８】図２６は、本発明の第３の実施例を示したものである。本実施例は、異なる管理ドメイン間移動時のＶＰＮ設定例（静的ＨＡ－ＣＮ間ＶＰＮ存在時）を示しており、ここでは、実施例１でローミング契約ＩＳＰ２のＦＡ２１から企業ドメインのＧＷ５１にＶＰＮが設定された後、ユーザのＭＮ１が異なるローミング契約ＩＳＰ２’の別のＦＡ２１’に移動した場合に、どのようにＶＰＮが再構築されるかを図式的に示している。

【００６９】図２６において、ユーザのＭＮ１は異なる管理ドメイン２－２’間を移動すると、ＤＩＡＭＥＴＥＲモバイルＩＰ拡張ドラフト（draft-ietf-calhoun-diameter-mobileip-08）に規定されているように、通常の初回位置登録と同じ手順で、登録要求（Ｒｅｇ　Ｒｅｑ）を送出する（①）。移動先のＦＡ２１’はこの登録要求を認証要求メッセージ（ＡＭＲ）に含め（②）、自ＩＳＰ内のローカルＡＡＡサーバ（ＡＡＡＦ）２２’を介して、ユーザのホームＩＳＰのＡＡＡ（ＡＡＡＨ）３３に送出する。

【0070】AAAH33は、VPN情報キャッシュにFA-HA，HA-企業GWの2つのVPNが設定済なので．FA-HAに関するVPNのFAを新FA21'のアドレスに書き換える。次に、HA31にこの2つのVPNのプロファイルを付加した位置登録要求メッセージ（HAR）を送信する（⑬）。HA31は、位置登録要求メッセージ（HAR）に付加されたVPN情報でキャッシュを更新し、HA31から旧FA21へのIPSecトンネルを削除後、新FA21'への新たなIPSecトンネル（1）を設定する。そして、位置登録処理終了後、位置登録応答メッセージ（HAA）をAAAHに返す（⑭）。この時、旧FA21のアドレスの情報を付加情報として返す。

【0071】AAAH33は位置登録応答メッセージ（HAA）を受信すると．VPN情報キャッシュからFA-HAのVPNを抽出し．FAに設定するこのVPNのプロファイルを付加した認証応答メッセージ（AMA）をAAAF23'へ送信する（⑮）。AAAF23'はMN1のローカルドメイン内での移動に対応するためVPN情報をAAAF内にキャッシュした後．それをFA21'に回送する。FA21'は、認証応答メッセージ（AMA）に付加されたVPN情報をキャッシュし．指定された差別化サービスのマッピングを行った後にFA21'からHA31へのIPSecトンネル（2）を設定する。また逆方向トンネルのパケットを復号するための情報をIPSec情報テーブルに設定する。

【0072】さらに、認証応答メッセージ（AMA）に旧FAのアドレスが含まれている場合はVPN情報キャッシュを複写し．送信元GWアドレスを旧FA21、宛先GWアドレスを新FA21'に書き換えた後にこのVPN情報をBUメッセージに付加して旧FA21に送信する（⑯）。旧FA21はBUメッセージに付加されたVPN情報をキャッシュし．FAからHAへのIPSecトンネルを削除し、指定された差別化サービスのマッピングを行った後にこのFA21から新FA21'へハンドオフ時のIPSecトンネル（3）を設定する。

【0073】その結果、HA31がIPSecトンネル（1）への切り替え前にMN1宛に旧FA21が受信したパケットは全てこのIPSecトンネル（3）を介して新FA21'へ回送される。FA21はIPSecトンネル（3）の設定完了後にBAメッセージを新FA21'に返す（⑰）。これにより、FA21'は登録応答メッセージ（Reg Rep）をMN1に返送する（⑱）。上述した実施例2及び3によれば、企業とISPを介して通信を行うユーザは、企業のGW装置に特殊な機能を持つことなく、ISPが提供するモバイル対応VPNのサービスを享受する事が可能となる。

【0074】図27は、本発明の第4の実施例を示したものである。本実施例は．初期位置登録時のVPN設定例（PCN存在時）を示しており、ここでは通信先のローミング契約ISPが動的にVPN設定可能なVPN GW（PCN）を配備している場合のVPN設定例を図式的に示している。動的にVPN設定可能なVPNGWを持つISPはISP間でローミング契約を結ぶときに．各々のプロバイダのCN-GW対応表にISPのドメインアドレスとGW装置アドレスを登録し、GW種別にVPN動的設定可を設定する。

【0075】図27において、これらのローミンググループのいずれかのISPに加入しているユーザは最寄りのアクセスポイントに接続し、そのMN1よりモバイルIPの位置登録要求（Reg Req）を送出する（①）。FA21はこの登録要求を認証要求メッセージ（AMR）に含めて自ISP内のローカルAAAサーバ（AAAF）23を介して．ユーザのホームISPのAAA（AAAH）33に送出する（②）。

【0076】AAAH33は、認証要求メッセージ（AMR）に含まれたNAIでVPNデータベース34を検索し．このユーザに固有のVPN情報を抽出する。VPNデータベース34にユーザ通信先として指定しているアドレスがローミング契約ISP4内であれば．CN-GWアドレス対応表からVPN動的設定可であることがわかるので、VPN情報キャッシュにFA-通信先ISP4のGW（PCN）41のVPNを設定する。HA31にこのVPNのプロファイルを付加した位置登録要求メッセージ（HAR）を送信する（③）。HA31は位置登録要求メッセージ（HAR）に付加されたVPN情報をキャッシュする。そして、位置登録処理終了後、VPN情報に設定された通信先GW41のGW種別を参照し．VPN動的設定可であるので、通信先端末CN42宛てにこのVPN情報を付加したMIP結合更新メッセージBUを送出する（④）。

【0077】PCN41は．CN42宛てに送出されたBUを代理受信し、BUに付加されたVPN情報をキャッシュする。通知されたVPN情報に従い差別化サービスのマッピングを行った後．PCN41からFA21へIPSecトンネル（1）を設定する。その後．MIP結合承認メッセージBAをHA31に送出する（⑤）。HA31はBAを受信すると位置登録応答メッセージ（HAA）をAAAH33に返す（⑥）。AAAH33は位置登録応答メッセージ（HAA）を受信すると、VPN情報キャッシュからFA-通信先ISP4のGW（PCN）のVPNを抽出し、FA21に設定するこのVPNのプロファイルを付加した認証応答メッセージ（AMA）をAAAF23へ送信する（⑦）。AAAF23はMN1のローカルドメイン内での移動に対応するためVPN情報をAAAF内にキャッシュした後．FA21に回送する。

【0078】FA21は認証応答メッセージ（AMA）に付加されたVPN情報をキャッシュし、指定された差

別化サービスのマッピングを行った後．ＦＡ２１からＰＣＮ４１へＩＰＳｅｃトンネル（２）を設定する。また逆方向トンネルのパケットを復号するための情報をＩＰＳｅｃ情報テーブルに設定する。その後、登録応答メッセージ（Ｒｅｇ　Ｒｅｐ）をＭＮに返す（⑧）。これにより．ローミング契約をしたＩＳＰグループ内であれば．ユーザは任意の通信先とＶＰＮ通信をすることできる。

【００７９】図２８は、本発明の第５の実施例を示したものである。本実施例は．同一ドメイン内移動時のＶＰＮ設定例（ＰＣＮ存在時）を示しており、ここでは実施例４でローミング契約ＩＳＰ２のＦＡ２１から任意のローミング契約ＩＳＰ４のＰＣＮ４１にＶＰＮが設定された後．ユーザのＭＮ１が同一ローミング契約ＩＳＰ２の別のＦＡ２１’に移動した場合に、どのようにＶＰＮが再構築されるかを図式的に示している。

【００８０】図２８において、ユーザのＭＮ１は同一ドメイン２内でＦＡ２１からＦＡ２１’へ移動すると、モバイルＩＰ経路最適化ドラフト（draft-ietf-mobileip-optim-09）に規定されているように．登録要求メッセージ（Ｒｅｇ　Ｒｅｑ）には旧ＦＡ２１のアドレスを含めて送出する（①）。新ＦＡ２１’はこの登録要求を認証要求メッセージ（ＡＭＲ）に含めて自ＩＳＰ内のローカルＡＡＡサーバ（ＡＡＡＦ）２３に送出する（②）。ＡＡＡＦ２３は．認証要求メッセージ（ＡＭＲ）に旧ＦＡ２１の情報が含まれている場合、ＶＰＮ情報キャッシュからＦＡ－ＰＣＮのＶＰＮを抽出し．ＦＡのアドレスを新ＦＡ２１’のアドレスに置換した後．ＦＡに設定するこのＶＰＮのプロファイルを付加した認証応答メッセージ（ＡＭＡ）を新ＦＡ２１’へ送信する（③）。

【００８１】ＦＡ２１’は先にＭＮ１から受信した登録要求メッセージ（Ｒｅｇ　Ｒｅｑ）をＨＡ３１に回送する（④）。ＨＡ３１はＶＰＮ情報キャッシュのうち、このＭＮ１が利用しているＶＰＮのＶＰＮプロファイルを特定し、ＦＡのアドレスを新ＦＡ２１’に書き換える。本実施例の場合．既にＶＰＮはＦＡ２１とＰＣＮ４１との間に直接設定されているため、その旨をＰＣＮ４１へＢＵメッセージで通知する（⑤）。なお、ＢＵメッセージを送出するか否かはＶＰＮ情報キャッシュの通信先ＧＷの種別が動的ＶＰＮ設定可であるかどうかで判定する。

【００８２】ＰＣＮ４１は．ＢＵの受信により旧ＦＡ２１へのＩＰＳｅｃトンネルを削除し．それに代えて新ＦＡ２１’へのＩＰＳｅｃトンネル（１）を設定する。その後．ＢＡメッセージをＨＡ３１に送信する（⑥）。ＨＡ３１はＢＡメッセージの受信により登録応答メッセージ（Ｒｅｇ　Ｒｅｐ）を新ＦＡ２１’に送信する（⑦）。新ＦＡ２１’はＶＰＮ情報キャッシュを参照して．指定された差別化サービスのマッピングを行った後．新ＦＡ２１’からＰＣＮ４１へＩＰＳｅｃトンネル

（２）を設定する。また逆方向トンネルのパケットを復号するための情報をＩＰＳｅｃ情報テーブルに設定する。更にＶＰＮ情報キャッシュを複写し、送信元ＧＷアドレスを旧ＦＡ２１、宛先ＧＷアドレスを新ＦＡ２１’に書き換えた後．このＶＰＮ情報をＢＵメッセージに付加して旧ＦＡ２１に送信する（⑧）。

【００８３】旧ＦＡ２１はＢＵメッセージに付加されたＶＰＮ情報をキャッシュし．旧ＦＡ２１からＰＣＮ４１へのＩＰＳｅｃトンネルを削除し、指定された差別化サービスのマッピングを行った後に旧ＦＡ２１から新ＦＡ２１’へスムースハンドオフ時のＩＰＳｅｃトンネル（３）を設定する。旧ＦＡ２１がＩＰＳｅｃトンネルへの切り替え前にＰＣＮ４１からＭＮ１宛に受信したパケットは全てこのＩＰＳｅｃトンネル（３）を介して新ＦＡ２１へ回送される。ＦＡ２１は、ＩＰＳｅｃトンネル設定完了後にＢＡメッセージを返送する（⑨）。新ＦＡ２１’は登録応答メッセージ（Ｒｅｇ　Ｒｅｐ）をＭＮ１に返送する（⑩’）。

【００８４】図２９は、本発明の第６の実施例を示したものである。本実施例は．異なる管理ドメイン間移動時のＶＰＮ設定例（ＰＣＮ存在時）を示しており．ここでは実施例４でローミング契約ＩＳＰ２のＦＡ２１から任意のローミング契約ＩＳＰ４のＰＣＮ４１にＶＰＮが設定された後、ユーザのＭＮ１が異なるローミング契約ＩＳＰ２’の別のＦＡ２１’に移動した場合に、どのようにＶＰＮが再構築されるかを図式的に示している。

【００８５】図２９において、ユーザのＭＮ１は異なる管理ドメイン間２－２’を移動すると．ＤＩＡＭＥＴＥＲモバイルＩＰ拡張ドラフト（draft-ietf-calhoun-diameter-mobileip-08）に規定されているように、通常の初回位置登録と同じ手順で登録要求メッセージ（Ｒｅｇ　Ｒｅｑ）を送出する（①）。ＦＡ２１’はこの登録要求を認証要求メッセージ（ＡＭＲ）に含めて自ＩＳＰ内のローカルＡＡＡサーバ（ＡＡＡＦ）２３’を介して、ユーザのホームＩＳＰのＡＡＡ（ＡＡＡＨ）３３に送出する（②）。ＡＡＡＨ３３は．ＶＰＮ情報キャッシュにＦＡ２１－ＰＣＮ４１のＶＰＮが設定済なので、このＦＡ２１のアドレスを新ＦＡ２１’のアドレスに書き換える。そして、ＨＡ３１にはこのＶＰＮのプロファイルを付加した位置登録要求メッセージ（ＨＡＲ）を送信する（③）。

【００８６】ＨＡ３１は．位置登録要求メッセージ（ＨＡＲ）に付加されたＶＰＮ情報でキャッシュを更新し、ＢＵメッセージをＰＣＮ４１へ送出する（④）。ＰＣＮ４１はＢＵメッセージを受信すると．旧ＦＡ２１へのＩＰＳｅｃトンネルを削除し．新ＦＡ２１’へＩＰＳｅｃトンネル（１）を設定する。その後．ＢＡメッセージをＨＡ３１に送信する（⑤）。ＨＡ３１はＢＡメッセージを受信すると位置登録応答メッセージ（ＨＡＡ）をＡＡＡＨ３３に返送する（⑥）。この時．旧ＦＡ２１のアド

レスの情報を付加情報として返す。

【００８７】ＡＡＡＨ３３は位置登録応答メッセージ（ＨＡＡ）を受信すると．ＶＰＮ情報キャッシュからＦＡ－ＰＣＮのＶＰＮを抽出し、ＦＡに設定するこのＶＰＮのプロファイルを付加した認証応答メッセージ（ＡＭＡ）をＡＡＡＦ２３’へ送信する（⑦）。ＡＡＡＦ２３’はＭＮ１のローカルドメイン内での移動に対応するためＶＰＮ情報をＡＡＡＦ内にキャッシュした後．それを新ＦＡ２１’に回送する。新ＦＡ２１’は認証応答メッセージ（ＡＭＡ）に付加されたＶＰＮ情報をキャッシュし．指定された差別化サービスのマッピングを行った後．新ＦＡ２１’からＰＣＮ４１へのＩＰＳｅｃトンネル（２）を設定する。また逆方向トンネルのパケットを復号するための情報をＩＰＳｅｃ情報テーブルに設定する。

【００８８】本例のように認証応答メッセージ（ＡＭＡ）に旧ＦＡ２１のアドレスが含まれている場合は、ＶＰＮ情報キャッシュを複写し、送信元ＧＷアドレスを旧ＦＡ２１．宛先ＧＷアドレスを新ＦＡ２１’に書き換えた後．このＶＰＮ情報をＢＵメッセージに付加して旧ＦＡ２１に送信する（⑧）。旧ＦＡ２１はＢＵメッセージに付加されたＶＰＮ情報をキャッシュし、旧ＦＡ２１からＰＣＮ４１へのＩＰＳｅｃトンネルを削除し．指定された差別化サービスのマッピングを行った後、このＦＡ２１から新ＦＡ２１’へスムーズハンドオフ時のＩＰＳｅｃトンネル（３）を設定する。

【００８９】ＩＰＳｅｃトンネルの切り替え前にＭＮ１宛にＰＣＮ４１から受信したパケットは全てこのＩＰＳｅｃトンネルを介して新ＦＡ２１’へ回送される。旧ＦＡ２１はＩＰＳｅｃトンネル（３）の設定完了後にＢＡメッセージをＭＮに返す（⑨）。それにより、新ＦＡ２１’は登録応答メッセージ（Ｒｅｇ　Ｒｅｐ）をＭＮ１に返送する（⑨’）。実施例５及び６に示すように、本発明によればローミング契約ＩＳＰグループに加入しているユーザはグループ内の任意の通信先とＶＰＮを設定でき．またＶＰＮを保持したままでグループ内を自由に移動することができる。

【００９０】図３０は、本発明の第７の実施例を示したものである。本実施例はユーザ指定の任意の端末間でのＶＰＮ設定例を示しており．これまではユーザが指定した特定の通信先に対してＶＰＮを設定する例を示したが．ユーザがＶＰＮを設定する通信先を動的に設定することもできる。この実施例では、ユーザが契約時に指定していた通信先以外の通信先にＶＰＮを設定する例を示す。

【００９１】ＶＰＮ設定先の変更を望むユーザは．ユーザのホームＩＳＰ３が提供するＶＰＮサービスカスタマイズ用のホームページにアクセスする。ユーザは．このホームページを介して、通信先のアドレスを設定する。このホームページと連動したＷＥＢアプリ３６はＶＰＮ

データベース３４の該ユーザのＶＰＮ情報をユーザが指定した情報に変更する（①）。ユーザのＭＮ１はカスタマイズが終了すると、サービス更新要求を付加した位置登録要求メッセージ（Ｒｅｇ　Ｒｅｑ）を現在接続しているＦＡ２１へ送出する（②）。ＦＡ２１はサービス更新要求が付加された登録要求を受信すると、この登録要求を認証要求メッセージ（ＡＭＲ）に含めて自ＩＳＰ内のローカルＡＡＡサーバ（ＡＡＡＦ）２３を介して、ユーザのホームＩＳＰのＡＡＡ（ＡＡＡＨ）３３に送出する（③）。

【００９２】ＡＡＡＨ３３は、ＶＰＮ情報キャッシュが既に存在するか否かに関係なくサービス更新要求が付加されたメッセージを受信すると、認証要求メッセージ（ＡＭＲ）に含まれたＮＡＩでＶＰＮデータベース３４を検索し、このユーザに固有のＶＰＮ情報を抽出する。ＶＰＮデータベース３４にユーザ通信先として指定しているアドレスがローミング契約ＩＳＰ内であれば．ＣＮ－ＧＷアドレス対応表からＶＰＮ動的設定可であることがわかるので．本例ではＶＰＮ情報キャッシュにＦＡ２１－通信先ＩＳＰのＧＷ（ＰＣＮ）４１’のＶＰＮを設定する。ＨＡ３１にこのＶＰＮのプロファイルを付加した位置登録要求メッセージ（ＨＡＲ）を送信する（④）。

【００９３】ＨＡ３１は．位置登録要求メッセージ（ＨＡＲ）に付加されたＶＰＮ情報をキャッシュする。位置登録処理終了後．ＶＰＮ情報に設定された通信先ＧＷ４１’のＧＷ種別を参照し．ＶＰＮ動的設定可であるので通信先端末ＣＮ４２’宛てにこのＶＰＮ情報を付加したＭＩＰ結合更新メッセージＢＵを送出する（⑤）。⑤ＰＣＮ４１’はＣＮ４２’宛てに送出されたＢＵを代理受信し．ＢＵメッセージに付加されたＶＰＮ情報をキャッシュする。通知されたＶＰＮ情報に従い差別化サービスのマッピングを行った後．ＰＣＮ４１’からＦＡ２１へのＩＰＳｅｃトンネル（１）を設定する。その後．ＭＩＰ結合承認メッセージＢＡをＨＡ３１に返送する。

【００９４】ＨＡ３１はＢＡメッセージを受信すると位置登録応答メッセージ（ＨＡＡ）をＡＡＡＨ３３に返す（⑦）。ＡＡＡＨ３３は位置登録応答メッセージ（ＨＡＡ）を受信すると、ＶＰＮ情報キャッシュからＦＡ２１－通信先ＩＳＰのＧＷ（ＰＣＮ）４１’のＶＰＮを抽出し．ＦＡ２１に設定するこのＶＰＮのプロファイルを付加した認証応答メッセージ（ＡＭＡ）をＡＡＡＦ２３へ送信する（⑧）。ＡＡＡＦ２３はＭＮ１のローカルドメイン内での移動に対応するためＶＰＮ情報をＡＡＡＦ内にキャッシュした後、それをＦＡ２１に回送する。

【００９５】ＦＡ２１は認証応答メッセージ（ＡＭＡ）に付加されたＶＰＮ情報をキャッシュし、指定された差別化サービスのマッピングを行った後．ＦＡ２１からＰＣＮ４１’へのＩＰＳｅｃトンネル（２）を設定する。また逆方向トンネルのパケットを復号するための情報を

ＩＰＳｅｃ情報テーブルに設定する。その後、登録応答メッセージ（Ｒｅｇ　Ｒｅｐ）をMNに返す（⑨）。ＶＰＮ変更前に設定されていたＶＰＮが存在していれば、ＶＰＮ情報を保持しているＰＣＮ４１はライフタイムの残り時間が閾値以下になった時、このＶＰＮ情報を通知してきたＨＡ３１へ結合要求メッセージＢＲを送出してＶＰＮを削除して良いか尋ねる（⑩）。

【００９６】ＨＡ３１はＢＲメッセージを受信すると、それに設定されたＭＮ１の情報からＶＰＮ情報キャッシュを検索し、このＰＣＮ４１に関するＶＰＮがまだキャッシュされているか調べる。キャッシュされていればＢＵメッセージをＰＣＮ４１へ送出する。キャッシュされていなければ何も送らない。本例ではＰＣＮ４１はライフタイム満了までにＢＵが受信されないため既存のＶＰＮを削除する。このように、ユーザが動的にＶＰＮ設定先を指定することもできる。本実施例では、単純にＷＥＢを介してＶＰＮ設定先を指定する例を示したが、本発明の本質は、モバイル環境での指定された設定先へのＶＰＮ情報の配布とその設定・解放手段であり、通信先の指定方法とそれに伴うＶＰＮデータベース３４への反映手段は様々なものが可能である。例えば、携帯電話による通信先とＶＰＮコードのダイヤルや、通信先サーバからの１クリックＶＰＮ設定等の応用例が考えられる。

【００９７】（付記１）モバイルＩＰネットワークにおけるＶＰＮシステムは、移動端末と、ユーザのホームネットワークに設けられたホーム認証サーバとそれ以外の外部ネットワークに設けられた外部認証サーバと、ホームネットワークに設けられたＶＰＮデータベースと、ホームネットワーク、外部ネットワーク、及び所定の通信ホスト及び／又はその代理サーバの各ゲートウェイ機能を有するネットワーク装置と、で構成され、ホーム認証サーバは、移動端末からの位置登録要求時に認証を要求したユーザのＶＰＮ情報をＶＰＮデータベースから抽出し、そのＶＰＮ情報を所定の位置登録メッセージ及び認証応答メッセージを用いて各ネットワーク装置に通知し、各ネットワーク装置は、通知されたＶＰＮ情報を基にホームネットワーク装置と外部ネットワーク装置間、ホームネットワーク装置と所定のネットワーク装置間、及び／又は外部ネットワーク装置と所定のネットワーク装置間にそれぞれＩＰＳｅｃによるＶＰＮパスを設定する、ことを特徴とするＶＰＮシステム。

（付記２）認証サーバ及びネットワーク装置は、移動端末の移動による位置登録要求と連動して認証サーバ及びネットワーク装置にキャッシュされたＶＰＮ情報を新経路情報に更新するか、又はモバイルＩＰで通知される位置情報で書き換えることにより、ホームネットワーク装置と外部ネットワーク装置間、ホームネットワーク装置と所定のネットワーク装置間、及び／又は外部ネットワーク装置と所定のネットワーク装置間の各ＶＰＮパスを新たなＩＰＳｅｃによるＶＰＮパスに自動更新する、付記１記載のシステム。

（付記３）さらに、外部認証サーバと外部ネットワーク装置間の所定の結合更新／承認メッセージにより、それらの間のスムースハンドオフ時にＩＰＳｅｃによるＶＰＮパスを設定する、付記２記載のシステム。

（付記４）ＶＰＮデータベースは、ユーザが所望するサービス品質、セキュリティゲートウェイ間のセキュリティ・サービス情報、及びＶＰＮを設定する通信先ホストのＩＰアドレス群からなるユーザ単位のＶＰＮ情報を格納する、付記１記載のシステム。

（付記５）ホーム認証サーバは、前記ＶＰＮデータベースのＶＰＮ情報と、自身が保有すると通信先ホストを収容する所定のネットワーク装置との対応表を用い、所定の認証要求メッセージに設定された移動端末が接続した外部ネットワーク装置の情報と移動端末のホームネットワーク装置の情報からＶＰＮ設定経路を特定するＡＡＡＶＰＮ制御部と、各ネットワーク装置間のサービス品質とセキュリティ情報をサービスプロファイルとして、アクセスネットワークへの所定の認証応答メッセージ及びホームネットワークへの位置登録メッセージに設定するＡＡＡプロトコル処理部と、を有する付記１記載の装置。

（付記６）各ネットワーク装置は、キャッシュによりＶＰＮ情報が設定されたサービスプロファイルに関連するプロトコル群を制御するＭＡプロトコル処理部と、そのサービスプロファイルに従ってサービス品質を保証するＱｏＳ制御とセキュリティゲートウェイ間のセキュリティを保証するためのトンネルを設定するＭＡＶＰＮ制御部と、を有する付記１記載の装置。

（付記７）ＭＡプロトコル処理部は、さらに配下のモバイルＩＰをサポートしない通信ホストに代わってホームネットワーク装置からの通信ホストへの結合更新メッセージを代理受信し、結合更新で通知されたＶＰＮ情報が設定されたサービスプロファイルを基に通信ホスト代わって他のネットワーク装置へのＩＰＳｅｃトンネルによるＶＰＮパスを設定するプロトコル処理を実行する、付記６記載のシステム。

（付記８）モバイルＩＰネットワークにおけるＶＰＮの設定方法は、

－　ユーザのネットワーク装置からそのホームエージェントに向けて静的なＩＰＳｅｃトンネルによるＶＰＮパスを設定すること、

－　ユーザの移動端末から外部エージェントに位置登録要求メッセージを送信すること、

－　外部エージェントは受信した位置登録要求情報を含む認証要求メッセージを、自身のローカル認証サーバを介してユーザのホーム認証サーバへ送信すること、

－　ホーム認証サーバは、受信した認証要求メッセージより自身のデータベースを参照して通信先ホスト、ネットワーク装置種別、及びユーザ別のセキュリティ・サー

ビス情報を抽出して外部－ホームエージェント間及びユーザのネットワーク装置－ホームエージェント間のＶＰＮ情報をキャッシュし、それらを含む位置登録要求メッセージをホームエージェントに送信すること、

－　ホームエージェントは、受信した位置登録要求メッセージをキャッシュし、指定されたセキュリティ・サービスを設定し、ホームエージェントから通信先ホストであるユーザのネットワーク装置及び外部エージェントに向けたＩＰＳｅｃトンネルによるＶＰＮパスを設定し、位置登録処理の終了後に位置登録応答メッセージをホーム認証サーバに送信すること、

－　ホーム認証サーバは、位置登録応答メッセージの受信により、キャッシュしてある外部－ホームエージェント間のＶＰＮ情報を付加した認証応答メッセージを外部エージェントのローカル認証サーバに送信すること、

－　ローカル認証サーバは、受信した認証応答メッセージをそのホーム－外部エージェント間のＶＰＮ情報をキャッシュしてから外部エージェントへ送信すること、

－　外部エージェントは、受信した認証応答メッセージに含まれるＶＰＮ情報をキャッシュし、指定されたセキュリティ・サービスを設定し、外部エージェントからホームエージェントに向けたＩＰＳｅｃトンネルによるＶＰＮパスを設定した後、ユーザの移動端末へ位置登録応答メッセージを返送すること、から成ることを特徴とするＶＰＮの設定方法。

（付記９）さらに、

－　ユーザの移動端末が同一ネットワーク内の新たな外部エージェントのエリアに移動し、そこから旧外部エージェントの位置情報を含む位置登録要求メッセージを送信すること、

－　新外部エージェントは受信した位置登録要求情報を含む認証要求メッセージを、ローカル認証サーバへ送信すること、

－　ローカル認証サーバは、キャッシュしてある外部－ホームエージェント間のＶＰＮ情報の外部エージェント情報を新外部エージェントの情報に書き換え、その情報を含む認証応答メッセージを新外部エージェントに送信すること、

－　新外部エージェントは、受信した位置登録要求メッセージをホームエージェントへ回送すること、

－　ホームエージェントは、受信した位置登録要求情報よりキャッシュしてある外部－ホームエージェント間のＶＰＮ情報の外部エージェント情報を新外部エージェントの情報に書き換え、ホームエージェントから旧外部エージェントに向けたＶＰＮパスを削除し、指定されたセキュリティ・サービスを設定したホームエージェントから新外部エージェントに向けたＩＰＳｅｃトンネルによるＶＰＮパスを設定し、位置登録処理の終了後に位置登録応答メッセージを新外部エージェントに送信すること。

－　新外部エージェントは、受信した位置登録応答メッセージに含まれるＶＰＮ情報をキャッシュし、指定されたセキュリティ・サービスを設定し、新外部エージェントからホームエージェントに向けたＩＰＳｅｃトンネルによるＶＰＮパスを設定した後、ユーザの移動端末へ位置登録応答メッセージを返送すること、を含む付記８記載の方法。

（付記１０）さらに、

－　ユーザの移動端末が別のネットワーク内の新たな外部エージェントのエリアに移動し、そこから旧外部エージェントの位置情報を含む位置登録要求メッセージを送信すること、

－　新外部エージェントは受信した位置登録要求情報を含む認証要求メッセージを、自身のローカル認証サーバを介してユーザのホーム認証サーバへ送信すること、

－　ホーム認証サーバは、受信した認証要求メッセージよりキャッシュしてある外部－ホームエージェント間のＶＰＮ情報の外部エージェント情報を新外部エージェントの情報に書き換え、その情報を含む位置登録要求メッセージをホームエージェントに送信すること、

－　ホームエージェントは、受信した位置登録要求情報によりキャッシュしてあるＶＰＮ情報を更新し、ホームエージェントから旧外部エージェントに向けたＶＰＮパスを削除し、指定されたセキュリティ・サービスを設定したホームエージェントから新外部エージェントに向けたＩＰＳｅｃトンネルによるＶＰＮパスを設定し、位置登録処理の終了後に位置登録応答メッセージをホーム認証サーバに送信すること、

－　ホーム認証サーバは、位置登録応答メッセージの受信により、キャッシュしてある外部－ホームエージェント間のＶＰＮ情報を付加した認証応答メッセージを新外部エージェントのローカル認証サーバに送信すること、

－　ローカル認証サーバは、受信した認証応答メッセージをキャッシュしてあるＶＰＮ情報を更新してから新外部エージェントへ回送すること、

－　新外部エージェントは、受信した認証応答メッセージに含まれるＶＰＮ情報をキャッシュし、指定されたセキュリティ・サービスを設定し、及び新外部エージェントからホームエージェントに向けたＩＰＳｅｃトンネルによるＶＰＮパスを設定した後、ユーザの移動端末へ位置登録応答メッセージを返送すること、を含む付記８記載の方法。

（付記１１）モバイルＩＰネットワークにおけるＶＰＮの設定方法は、

－　ユーザの移動端末から外部エージェントに位置登録要求メッセージを送信すること、

－　外部エージェントは受信した位置登録要求情報を含む認証要求メッセージを、自身のローカル認証サーバを介してユーザのホーム認証サーバへ送信すること、

－　ホーム認証サーバは、受信した認証要求メッセージ

より自身のデータベースを参照して通信先ホスト．ネットワーク装置種別、及びユーザ別のセキュリティ・サービス情報を抽出し、ネットワーク装置種別がＶＰＮ動的設定可である場合はＶＰＮキャッシュに外部エージェント－通信先ネットワーク装置のＶＰＮを設定して．それらの情報を含む位置登録要求メッセージをホームエージェントに送信すること、

－　ホームエージェントは．受信した位置登録要求メッセージをキャッシュし、位置登録処理の終了後にネットワーク装置種別がＶＰＮ動的設定可である場合は通信先ホスト宛にこのＶＰＮ情報を付加した結合更新メッセージを送出すること、

－　ネットワーク装置は結合更新メッセージを代理受信し．それに付加されたＶＰＮ情報をキャッシュし．指定されたセキュリティ・サービスを設定し、ネットワーク装置から外部エージェントに向けたＩＰＳｅｃトンネルによるＶＰＮパスを設定し．その後に結合承認メッセージをホームエージェントに送信すること、

－　ホームエージェントは．結合承認メッセージを受信すると、位置登録応答メッセージをホーム認証サーバへ送信すること．

－　ホーム認証サーバは．位置登録応答メッセージの受信により、キャッシュしてある外部エージェント－ネットワーク装置間のＶＰＮ情報を付加した認証応答メッセージを外部エージェントのローカル認証サーバに送信すること、

－　ローカル認証サーバは．受信した認証応答メッセージをその付加されたＶＰＮ情報をキャッシュしてから外部エージェントへ送信すること、

－　外部エージェントは．受信した認証応答メッセージに含まれるＶＰＮ情報をキャッシュし．指定されたセキュリティ・サービスを設定し、外部エージェントからネットワーク装置に向けたＩＰＳｅｃトンネルによるＶＰＮパスを設定した後、ユーザの移動端末へ位置登録応答メッセージを返送すること．から成ることを特徴とするＶＰＮの設定方法。

（付記１２）さらに、

－　ユーザの移動端末が同一ネットワーク内の新たな外部エージェントのエリアに移動し、そこから旧外部エージェントの位置情報を含む位置登録要求メッセージを送信すること、

－　新外部エージェントは受信した位置登録要求情報を含む認証要求メッセージを．ローカル認証サーバへ送信すること、

－　ローカル認証サーバは．キャッシュしてある外部エージェント－ネットワーク装置間のＶＰＮ情報の外部エージェント情報を新外部エージェントの情報に書き換え．その情報を含む認証応答メッセージを新外部エージェントに送信すること、

－　新外部エージェントは．受信した位置登録要求メッセージをホームエージェントへ回送すること、

－　ホームエージェントは．受信した位置登録要求情報よりキャッシュしてある外部エージェント－ネットワーク装置間のＶＰＮ情報の外部エージェント情報を新外部エージェントの情報に書き換え、ネットワーク装置種別がＶＰＮ動的設定可である場合は通信先ホスト宛にこのＶＰＮ情報を付加した結合更新メッセージを送出すること．

－　ネットワーク装置は受信した結合更新メッセージよりキャッシュしてあるＶＰＮ情報を更新し、ネットワーク装置から旧外部エージェントに向けたＶＰＮパスを削除し．指定されたセキュリティ・サービスを設定したネットワーク装置から新外部エージェントに向けたＩＰＳｅｃトンネルによるＶＰＮパスを設定し、その後に結合承認メッセージをホームエージェントに送信すること、

－　ホームエージェントは．結合承認メッセージを受信すると、位置登録応答メッセージを新外部エージェントへ送信すること．

－　新外部エージェントは．受信した位置登録応答メッセージに含まれるＶＰＮ情報をキャッシュし、指定されたセキュリティ・サービスを設定し．新外部エージェントからネットワーク装置に向けたＩＰＳｅｃトンネルによるＶＰＮパスを設定した後、ユーザの移動端末へ位置登録応答メッセージを返送すること．を含む付記１１記載の方法。

（付記１３）さらに、

－　ユーザの移動端末が別のネットワーク内の新たな外部エージェントのエリアに移動し、そこから旧外部エージェントの位置情報を含む位置登録要求メッセージを送信すること、

－　新外部エージェントは受信した位置登録要求情報を含む認証要求メッセージを．自身のローカル認証サーバを介してユーザのホーム認証サーバへ送信すること、

－　ホーム認証サーバは．受信した認証要求メッセージよりキャッシュしてある外部エージェント－ネットワーク装置間のＶＰＮ情報の外部エージェント情報を新外部エージェントの情報に書き換え、その情報を含む位置登録要求メッセージをホームエージェントに送信すること．

－　ホームエージェントは．受信した位置登録要求情報によりキャッシュしてあるＶＰＮ情報を更新し．ネットワーク装置種別がＶＰＮ動的設定可である場合は通信先ホスト宛にこのＶＰＮ情報を付加した結合更新メッセージを送出すること、

－　ネットワーク装置は受信した結合更新メッセージよりキャッシュしてあるＶＰＮ情報を更新し、ネットワーク装置から旧外部エージェントに向けたＶＰＮパスを削除し．指定されたセキュリティ・サービスを設定したネットワーク装置から新外部エージェントに向けたＩＰＳｅｃトンネルによるＶＰＮパスを設定し、その後に結合

承認メッセージをホームエージェントに送信すること、

－　ホームエージェントは、結合承認メッセージを受信すると、位置登録応答メッセージをホーム認証サーバへ送信すること、

－　ホーム認証サーバは、位置登録応答メッセージの受信により、キャッシュしてある外部エージェント－ネットワーク装置間のＶＰＮ情報を付加した認証応答メッセージを新外部エージェントのローカル認証サーバに送信すること、

－　ローカル認証サーバは、受信した認証応答メッセージをその付加されたＶＰＮ情報をキャッシュしてから新外部エージェントへ回送すること、

－　新外部エージェントは、受信した認証応答メッセージに含まれるＶＰＮ情報をキャッシュし、指定されたセキュリティ・サービスを設定し、新外部エージェントからネットワーク装置に向けたＩＰＳｅｃトンネルによるＶＰＮパスを設定した後、ユーザの移動端末へ登録応答メッセージを返送すること、を含む付記１１記載の方法。

（付記１４）さらに、

－　新外部エージェントは、キャッシュしてあるＶＰＮ情報を複写して、送信元を旧外部エージェント及び送信先を新外部エージェントに書き換えたＶＰＮ情報を付加した結合更新メッセージを旧外部エージェントへ送信すること、

－　旧外部エージェントは、受信した結合更新メッセージのＶＰＮ情報をキャッシュし、旧外部エージェントからホームエージェントに向けたＶＰＮパスを削除し、指定されたセキュリティ・サービスを設定した旧外部エージェントから新外部エージェントに向けたＩＰＳｅｃトンネルによるＶＰＮパスを設定した後、新外部エージェントへ結合承認メッセージを送信すること、を含む付記９又は１２記載の方法。

（付記１５）さらに、

－　新外部エージェントは、認証応答メッセージに旧外部エージェントの情報が含まれている時は、キャッシュしてあるＶＰＮ情報を複写して、送信元を旧外部エージェント及び送信先を新外部エージェントに書き換えたＶＰＮ情報を付加した結合更新メッセージを旧外部エージェントへ送信すること、

－　旧外部エージェントは、受信した結合更新メッセージのＶＰＮ情報をキャッシュし、旧外部エージェントからホームエージェントに向けたＶＰＮパスを削除し、指定されたセキュリティ・サービスを設定した旧外部エージェントから新外部エージェントに向けたＩＰＳｅｃトンネルによるＶＰＮパスを設定した後、新外部エージェントへ結合確認メッセージを送信すること、を含む付記１０又は１３記載の方法。

（付記１６）さらに、

－　ユーザが所定の通信手段によりそのホーム認証サーバのデータベースへアクセスしてユーザのＶＰＮ情報をカスタマイズし、それによりネットワーク装置種別がＶＰＮ動的設定可であるネットワーク装置に通信先を変更すること、

－　ユーザの移動端末から外部エージェントにサービス更新要求を付加した位置登録要求メッセージを送信すること、を含む付記１１記載の方法。

（付記１７）さらに、

－　ネットワーク装置は配下の通信ホストのライフタイムを計測し、残りのライフタイムが所定閾値以下になった時にそのＶＰＮ情報を通知してきたホームエージェントに結合要求メッセージを送信し、結合更新メッセージを受信しない場合には前記ＶＰＮ情報を削除すること、

－　ホームエージェントは受信した結合要求メッセージに含まれるユーザの移動端末の情報からキャッシュしてあるＶＰＮ情報を検索し、前記ネットワーク装置の情報が存在する場合は結合更新メッセージを送信し、存在しない場合には放置すること、を含む付記１６記載の方法。

【００９８】

【発明の効果】以上説明したように、本発明によれば以下に示す効果が奏される。

１）モバイルＩＰにおける位置登録手順に連携して、通信に関与する端末の公衆ＩＰネットワークへのセキュリティゲートウェイに動的にＩＰＳｅｃを用いたＶＰＮを設定する事で、ＭＮやＣＮにＶＰＮ用の特殊な機能を持たせる事無しに、任意の端末間でのＶＰＮ設定サービスの提供を可能にする。

２）ユーザが自由に組み合わせて指定したサービス品質、セキュリティレベル、経路でのＶＰＮ設定を可能にする。

３）ＭＮの移動に伴い、ＶＰＮの経路を自動更新することを可能にする。

【図面の簡単な説明】

【図１】既存提案によるモバイルＩＰ＋ＩＰＳｅｃの適用例を示した図である。

【図２】本発明によるネットワーク構成の一例を示した図である。

【図３】本発明の機能ブロック構成例を示した図である。

【図４】本発明の第１の実施例を示した図である。

【図５】ＶＰＮデータベースの構成例を示した図である。

【図６】ＡＡＡの詳細機能ブロック構成例を示した図である。

【図７】ＶＰＮ情報キャッシュの構成例を示した図である。

【図８】ＣＮ－ＧＷアドレス対応表を示した図である。

【図９】ＡＡＡの全体処理フロー例を示した図である。

【図１０】ＡＡＡプロトコル処理部の処理フロー例を示

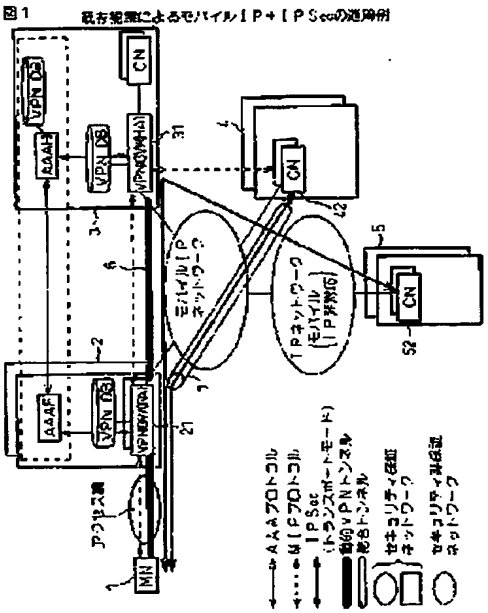
33

した図である。
【図１１】図１０でのメッセージ対応表を示した図である。
【図１２】ＡＡＡＶＰＮ制御部の処理フロー例を示した図である。
【図１３】ＶＰＮ経路決定制御部の処理フロー例を示した図である。
【図１４】ＭＡ（ＦＡ，ＨＡ，ＰＣＮ）の詳細機能ブロック例を示した図である。
【図１５】ＩＰＳｅｃ情報テーブルの構成例を示した図である。
【図１６】ルートテーブルの構成例を示した図である。
【図１７】ＭＡの全体処理フロー例を示した図である。
【図１８】ＭＡプロトコル処理部の処理フロー例を示した図である。
【図１９】ＡＡＡプロトコル処理部の処理フロー例を示した図である。
【図２０】モバイルＩＰプロトコル処理部の処理フロー例を示した図である。
【図２１】図２０でのメッセージ対応表を示した図である。

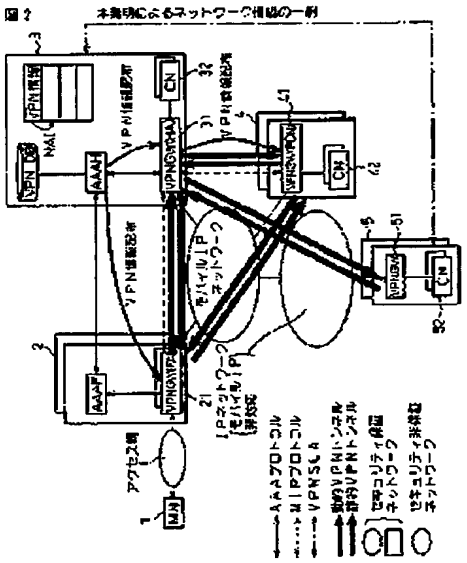
34

＊る。
【図２２】ＭＡＶＰＮ制御部の処理フロー例を示した図である。
【図２３】ＱｏＳ制御部の処理フロー例を示した図である。
【図２４】トンネル制御部の処理フロー例を示した図である。
【図２５】本発明の第２の実施例を示した図である。
【図２６】本発明の第３の実施例を示した図である。
【図２７】本発明の第４の実施例を示した図である。
【図２８】本発明の第５の実施例を示した図である。
【図２９】本発明の第６の実施例を示した図である。
【図３０】本発明の第７の実施例を示した図である。
【符号の説明】
１…モバイルノード
２～５…ＩＳＰネットワーク
２１．３１、４１、５１…セキュリティゲートウェイ
２３．３３…ＡＡＡ認証サーバ
３４…ＶＰＮデータベース
３６…ウェブアプリケーション

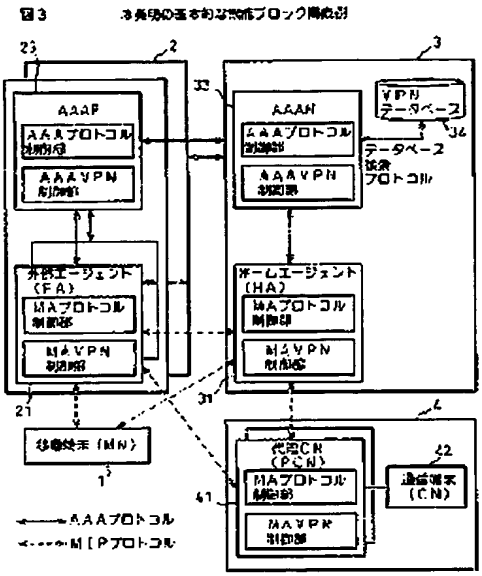
【図１】



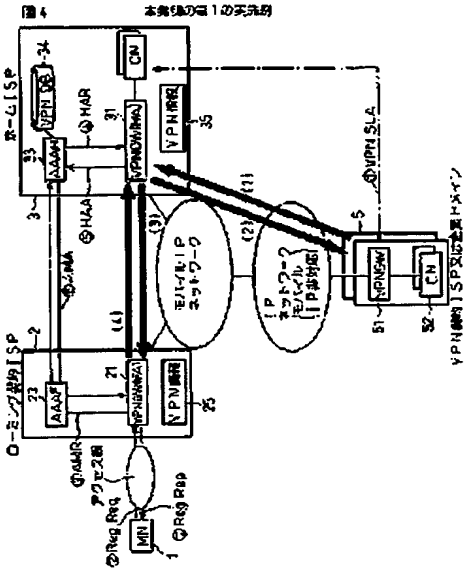
【図２】



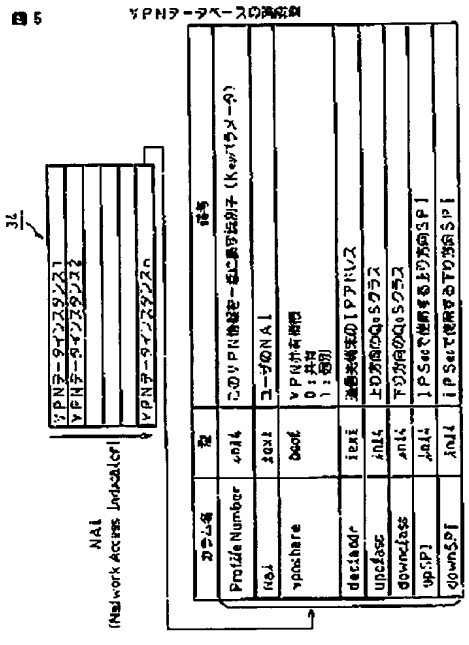
【図３】



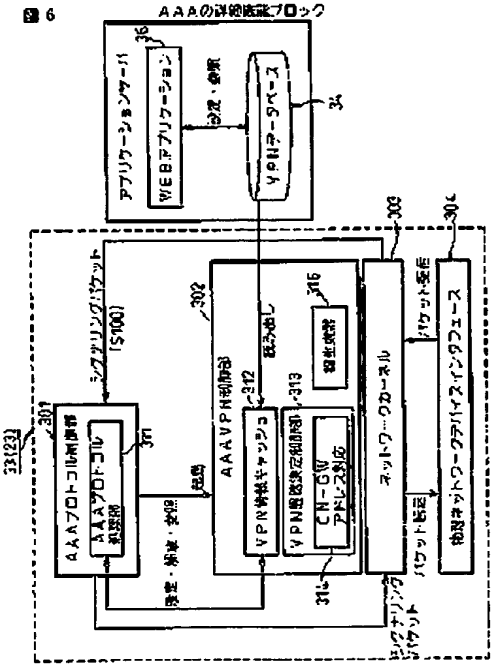
【図４】



【図５】

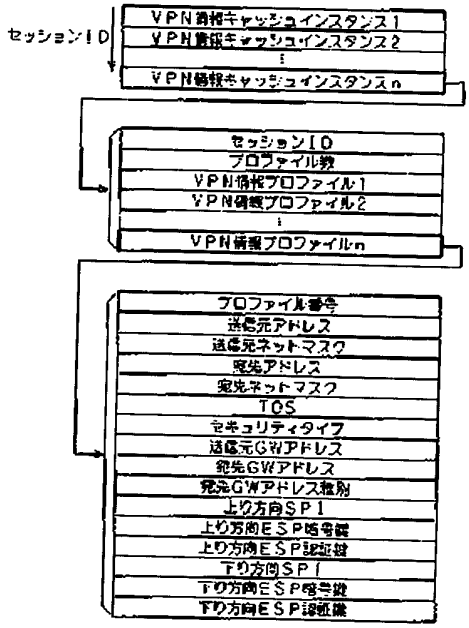


【図６】



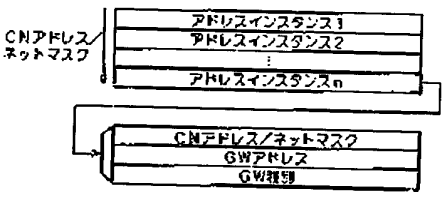
【図７】

図７ VPN情報キャッシュの一例



【図８】

図８ CN－GWアドレス対応表の一例



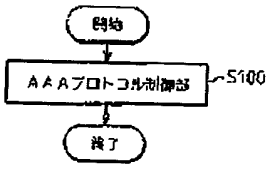
【図１１】

図11 図6のS103でのメッセージ対応表

受信メッセージ	処理実行AAA	送信メッセージ
AMR	AAAF	AMR
	AAAH	HAR
AMA	AAAF	AMA
HAA	AAAH	AMA

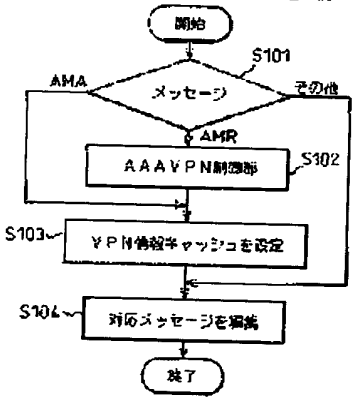
【図９】

図９ AAA全体処理フロー例



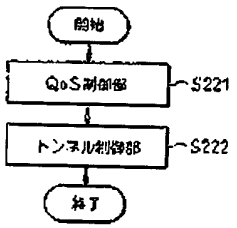
【図１０】

図10 AAAプロトコル処理部の処理フロー例

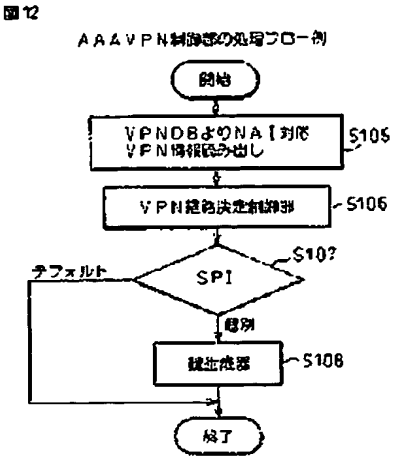


【図２２】

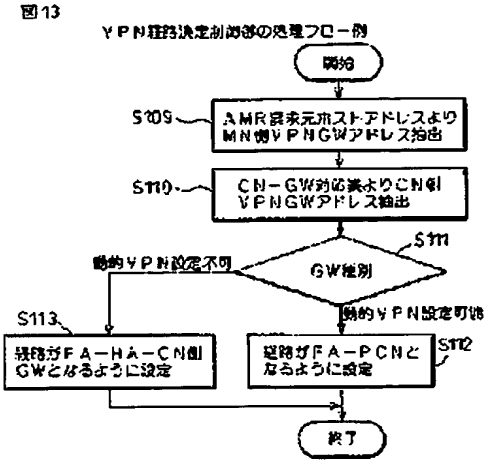
図22 MAVPN制御部の処理フロー例



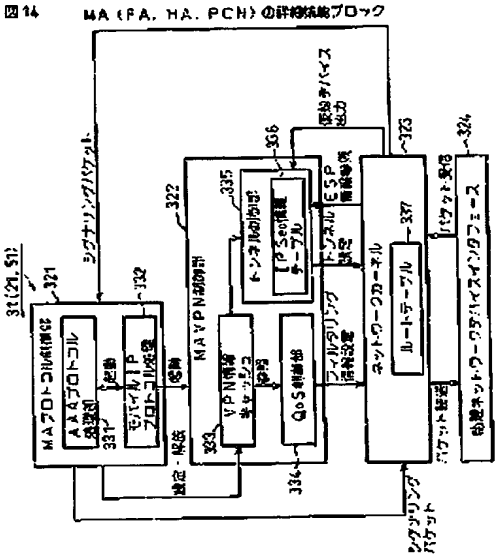
【図１２】



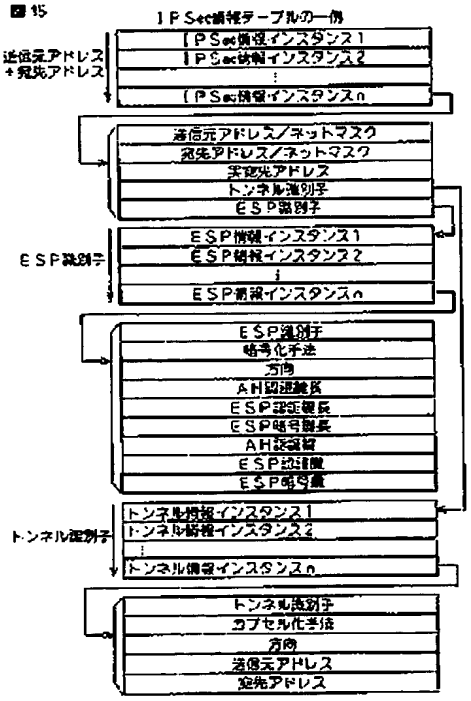
【図１３】



【図１４】

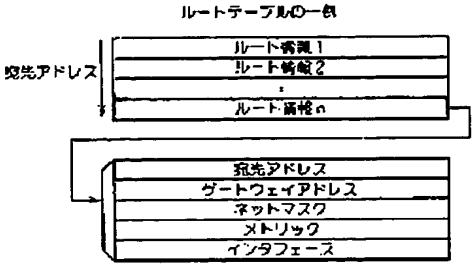


【図１５】



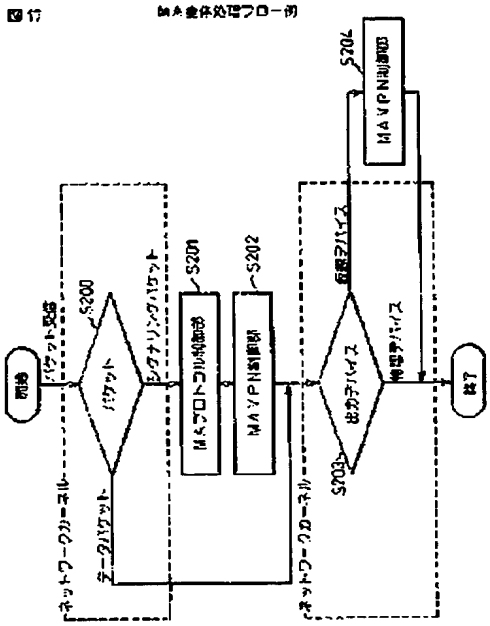
【図１６】

図16



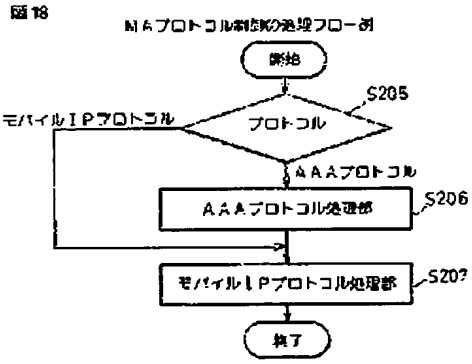
【図１７】

図17



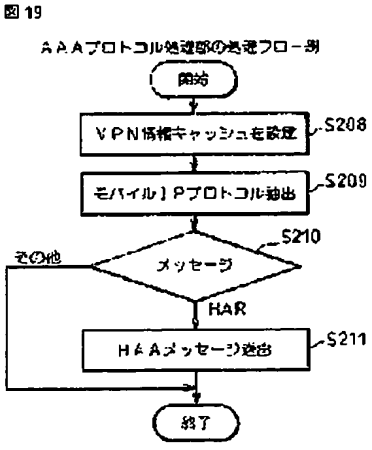
【図１８】

図18



【図１９】

図19



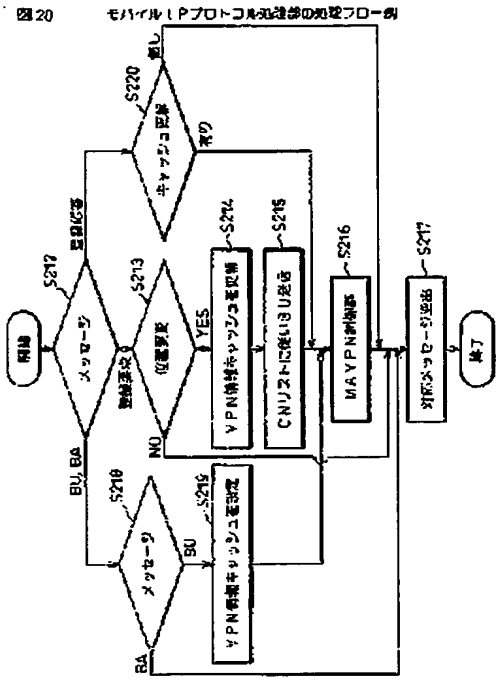
【図２１】

図21

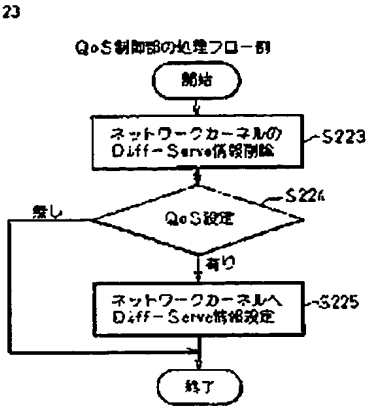
図20のS217でのメッセージ対応表

受信メッセージ	処理実行MA	送信メッセージ
登録要求	FA	登録応答
	HA	BU
登録応答	FA	登録応答
BU	FA,PCN	BA
BA	HA	登録応答

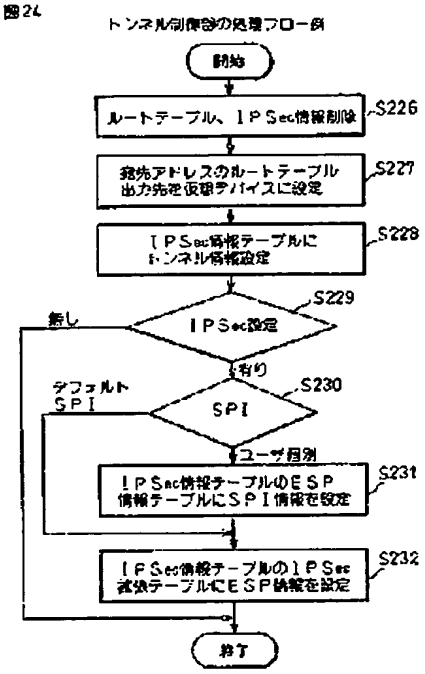
【図２０】



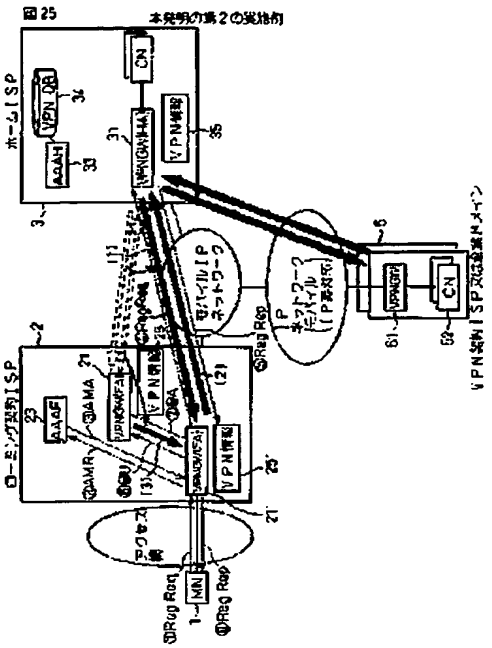
【図２３】



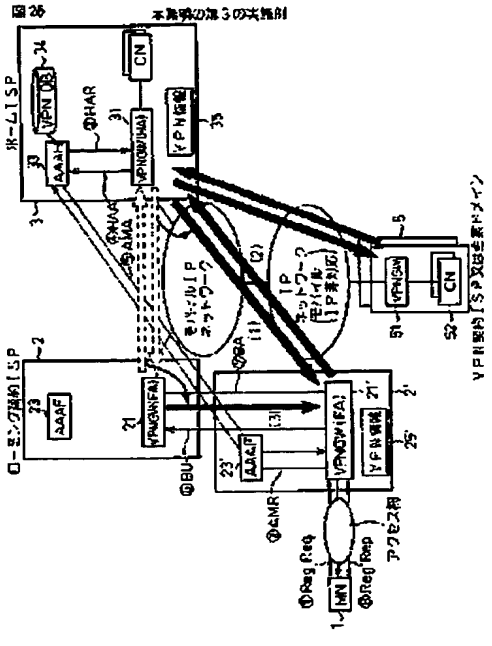
【図２４】



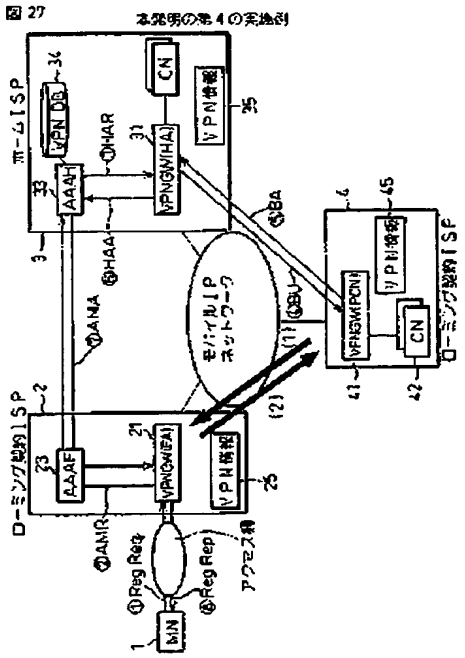
【図25】



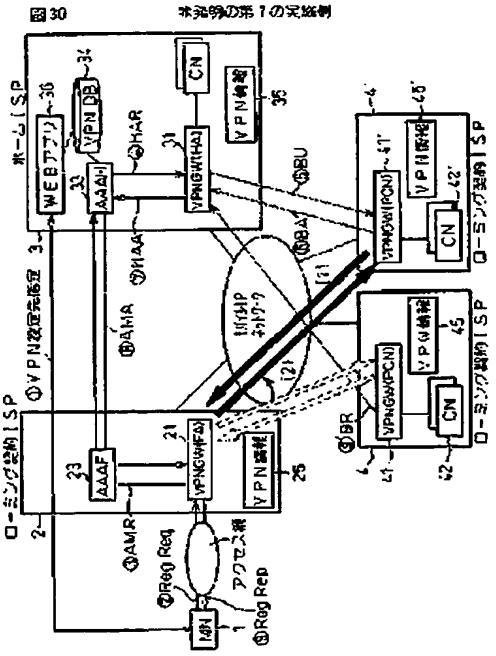
【図26】



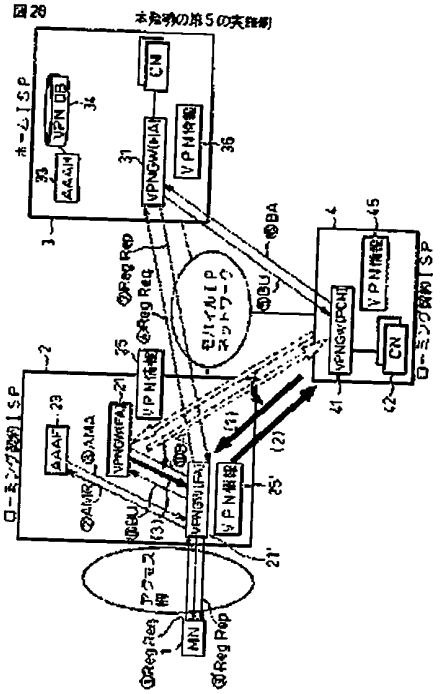
【図27】



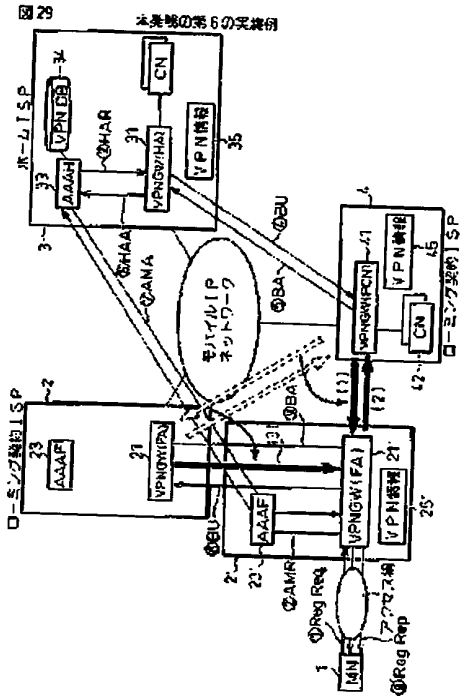
【図30】



【図２８】



【図２９】



フロントページの続き

(72)発明者　五十嵐　洋一郎
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　村田　一徳
福岡県福岡市早良区百道浜２丁目２番１号　富士通西日本コミュニケーション・システムズ株式会社内
(72)発明者　若本　雅晶
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

Ｆターム(参考)　5K030 GA15 HA08 HC01 HC09 HD03 JA01 JL01 JL07 JT03 JT09 KA07 KA13 LA08 LB01 LC06 LD19 MA06